



БИБЛИОТЕЧКА • КВАНТ •
выпуск 3

О. ОРЕ

ПРИГЛАШЕНИЕ В ТЕОРИЮ ЧИСЕЛ







БИБЛИОТЕЧКА • КВАНТ •
выпуск 3

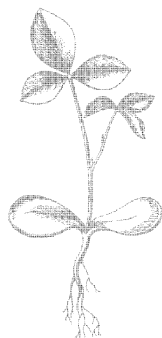
О. ОРЕ

ПРИГЛАШЕНИЕ В ТЕОРИЮ ЧИСЕЛ

Перевод с английского
Л. А. САВИНОЙ и А. П. САВИНА



МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1980



Scan AAW

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Академик И. К. Кикоин (председатель), академик А. Н. Колмогоров (заместитель председателя), кандидат физ.-мат. наук И. Ш. Слободский (ученый секретарь), член-корреспондент АН СССР А. А. Абрикосов, академик Б. К. Вайнштейн, заслуженный учитель РСФСР Б. В. Воздвиженский, академик В. М. Глушков, академик П. Л. Капица, профессор С. П. Капица, член-корреспондент АН СССР Ю. А. Осипьян, член-корреспондент АПН СССР В. Г. Разумовский, академик Р. З. Сагдеев, кандидат хим. наук М. Л. Смолянский, профессор Я. А. Смородинский, академик С. Л. Соболев, член-корреспондент АН СССР Д. К. Фаддеев, член-корреспондент АН СССР И. С. Шкловский.

Оре О.

О 65 Приглашение в теорию чисел: Пер. с англ. → М.: Наука. Главная редакция физико-математической литературы, 1980. — 128 с илл. — (Библиотека «Квант». Вып. 3): 30 к.

Книга известного норвежского математика О. Оре раскрывает красоту математики на примере одного из ее старейших разделов — теории чисел. Изложение основ теории чисел в книге во многом нетрадиционно. Наряду с теорией сравнений, сведениями о системах счисления, в ней содержатся рассказы о магических квадратах, о решении арифметических ребусов и т. д. Большим достоинством книги является то, что автор при каждом удобном случае указывает на возможности практического применения изложенных результатов, а также знакомит читателя с современным состоянием теории чисел и задачами, еще не получившими окончательного решения.

О $\frac{20203-081}{053(02)-80}$ 90-80. 1702030000

ББК22.13Г
517.1

О $\frac{20203-081}{053(02)-80}$ 90-80. 1702030000

© Издательство «Наука». Главная редакция физико-математической литературы, перевод на русский язык, 1980

ОГЛАВЛЕНИЕ

От переводчиков	7
Глава 1. ВВЕДЕНИЕ	9
§ 1. История	9
§ 2. Нумерология	9
§ 3. Задача Пифагора	10
§ 4. Фигурные числа	12
§ 5. Магические квадраты	15
Глава 2. ПРОСТЫЕ ЧИСЛА	23
§ 1. Простые и составные числа	23
§ 2. Простые числа Мерсенна	26
§ 3. Простые числа Ферма	29
§ 4. Решето Эратосфена	32
Глава 3. ДЕЛИТЕЛИ ЧИСЕЛ	35
§ 1. Основная теорема о разложении на множители	35
§ 2. Делители	38
§ 3. Несколько задач о делителях	40
§ 4. Совершенные числа	42
§ 5. Дружественные числа	44
Глава 4. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ И НАИ- МЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ	47
§ 1. Наибольший общий делитель	47
§ 2. Взаимно простые числа	49
§ 3. Алгоритм Евклида	51
§ 4. Наименьшее общее кратное	54
Глава 5. ЗАДАЧА ПИФАГОРА	57
§ 1. Предварительные замечания	57
§ 2. Решение задачи Пифагора	58
§ 3. Несколько задач о треугольниках Пифагора	61
Глава 6. СИСТЕМЫ СЧИСЛЕНИЯ	70
§ 1. Числа	70
§ 2. Другие системы	71
§ 3. Сравнение систем счисления	75
§ 4. Некоторые задачи, связанные с системами счисления	80
§ 5. Компьютеры и их системы счисления	83
§ 6. Игры с числами	85

Г л а в а 7. СРАВНЕНИЯ	90
§ 1. Определение сравнения	90
§ 2. Некоторые свойства сравнений	91
§ 3. Алгебра сравнений	94
§ 4. Возведение сравнений в степень	96
§ 5. Теорема Ферма	99
Г л а в а 8. НЕКОТОРЫЕ ПРИМЕНЕНИЯ СРАВНЕНИЙ	103
§ 1. Проверка вычислений	103
§ 2. Дни недели	108
§ 3. Расписания соревнований	114
§ 4. Простое или составное?	117
РЕШЕНИЯ ИЗБРАННЫХ ЗАДАЧ	120
ЗАКЛЮЧЕНИЕ	127

Имя О. Оре (1899—1968) хорошо известно у нас в стране. Две его книги по теории графов, переведенные на русский язык (О. Оре. Теория графов. — М.: Наука. 1968 и Графы и их применение. — М.: Мир, 1965) были тепло встречены читателями в СССР. С большим интересом был принят и перевод его книги о Нильсе Абеле (О. Оре. Замечательный математик Нильс Хенрик Абель. — М.: Физматгиз, 1961.)

Предлагаемая читателю книга О. Оре «Приглашение в теорию чисел» относится к чрезвычайно редкостному типу научно-популярных книг. Как правило, научно-популярные книги по математике имеют своей целью научить читателя чему-либо или дать ему представление о той или иной ветви математики. О. Оре не ставит перед собой ни той, ни другой задачи. Его цель — заинтересовать читателя математикой (а читателем предполагается школьник 13—17 лет), привить ему вкус к этой древней, но вечно юной науке.

Оре рассказывает о магических квадратах и числовых ребусах, вычислении дней недели и составлении расписаний соревнований — вещах либо интригующих, либо имеющих реальное практическое значение. В результате, если читатель и не захочет стать математиком (а ими становятся единицы), то он надолго сохранит впечатление о красоте математики, силе и широте диапазона применений ее на практике.

Написанная просто и доступно, эта книга (за исключением нескольких страниц) может быть легко прочитана школьником начиная с 5—6 класса. Поскольку этот перевод адресован в первую очередь школьникам, то переводчики сочли необходимым полностью сменить рекомендуемую литературу на книги, доступные этой категории читателей.

ВВЕДЕНИЕ

§ 1. История

Теория чисел — это ветвь математики, имеющая дело с *целыми положительными числами*

1, 2, 3, ...,

которые также называют *натуральными числами*.

Археология и история учат нас, что человек рано начал считать. Сначала он научился складывать числа, потом, много позже, умножать и вычитать их. Деление чисел было необходимым для распределения на равные части кучи яблок или улова рыбы. Эти действия над числами называются *вычислениями*. В некоторых случаях последовательность вычислений называют «калькуляцией». Это слово происходит от латинского *calculus*, означающего «маленький камень», поскольку римляне пользовались морской галькой при вычислениях на своих счетных досках.

Как только люди немного научились считать, этот процесс стал приятным времяпровождением для многих людей, склонных к абстрактному теоретизированию. Знания о числах накапливались в течение многих веков, порождая интерес к новым исследованиям, которые в свою очередь приумножали эти накопления. И сейчас, в современной математике, мы имеем величественную конструкцию, известную как теория чисел. Некоторые части этой теории все еще составляют простые игры с числами, а другие относятся к наиболее трудным и сложным разделам математики.

§ 2. Нумерология

Некоторые следы размышлений о числах в давние времена можно обнаружить в суеверных предрассудках, связанных с числами. Среди чисел

есть «счастливые», которым нужно отдавать предпочтение и радоваться при встрече с ними, и «несчастливые», которых нужно остерегаться, как дурного глаза. Мы обладаем обширными сведениями о *нумерологии* в античной Греции, мыслях и предрассудках, связанных с символическим значением различных чисел. Например, нечетные числа, большие единицы, символизировали мужское начало, а четные — женское; таким образом, число 5 — сумма первого мужского и первого женского чисел — символизировало супружество или союз.

Желающие познакомиться с более развитой «теорией» магических чисел могут сделать это, прочтя восьмую книгу «Республики» Платона. Такая «наука» мало что дает в смысле математических идей, но она содержит умение обращаться с числами и их свойствами. Как мы дальше увидим, некоторые замечательные проблемы в теории чисел, до сих пор занимающие умы математиков, берут свое начало из греческого учения о магических числах.

До сих пор у нас нет оснований считать себя выше предрассудков, связанных с числами. Вероятно, у каждого есть знакомые, которые ни за что не посадят за стол 13 гостей, а как мало в гостиницах США этажей и комнат с номером 13. По существу, мы не знаем, откуда взялись подобные «табу» на числа. Существует множество всевозможных объяснений, но большинство из них совершенно безосновательны. Например, в «Библии» записано, что на Тайной вечере было 13 гостей, разумеется, тринадцатым был Иуда. Если же заметить, что многие предметы считаются дюжинами, а число 13 дает «чертову дюжину», т. е. лишний предмет, то это соображение имеет больший реальный смысл.

В «Библии», особенно в «Ветхом Завете», особую роль играет число 7, в древнегерманском фольклоре часто встречаются числа 3 и 9, индусы же, как видно из их мифологии, равнодушны к числу 10.

§ 3. Задача Пифагора

Примером ранней теории чисел может служить *задача Пифагора*. Как мы знаем, в прямоугольном треугольнике длины сторон удовлетворяют

соотношению Пифагора

$$z^2 = x^2 + y^2, \quad (1.3.1)$$

где z — длина гипотенузы. Это дает возможность в прямоугольном треугольнике вычислить длину одной стороны, если известны две другие. Между прочим, то, что эту теорему называли в честь греческого философа Пифагора, не совсем справедливо: она была известна вавилонянам почти за 2000 лет до Пифагора.

Иногда все длины сторон x , y , z в (1.3.1) выражаются целыми числами. Простейший случай,

$$x = 3, \quad y = 4, \quad z = 5, \quad (1.3.2)$$

был найден на вавилонских глиняных табличках. Этому случаю можно дать следующее истолкование. Предположим, что у нас

есть веревочное кольцо с узелками или метками, расположенными на равных расстояниях и делящими кольцо на 12 частей. Тогда, если мы растянем кольцо на трех кольях, вбитых на поле, так, чтобы получился тре-

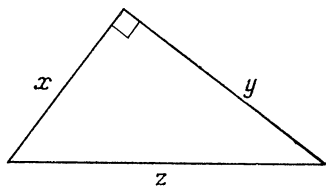


Рис. 1.

угольник со сторонами 3 и 4, то третья сторона будет иметь длину 5, а противоположный ей угол будет прямым (рис. 1). Часто можно прочесть в книгах по истории математики, что именно этот метод построения прямого угла использовался египетскими землемерами или «натягивателями веревки» при размежевании полей по окончании разлива Нила. Однако вполне возможно, что это один из мифов, которых так много в истории науки; у нас нет документов, подтверждающих это предположение.

Существует много других целочисленных решений уравнения Пифагора (1.3.1), например,

$$x = 5, \quad y = 12, \quad z = 13,$$

$$x = 7, \quad y = 24, \quad z = 25,$$

$$x = 8, \quad y = 15, \quad z = 17.$$

Далее мы покажем, как можно получить все такие решения. Способ находить их был известен древним грекам, а возможно, и вавилонянам.

Если даны два целых числа, x и y , то всегда можно найти соответствующее число z , удовлетворяющее уравнению (1.3.1), но вполне возможно, что z будет иррациональным числом. Если же потребовать, чтобы все три числа были целыми, то тогда возможности существенно ограничиваются. Греческий математик Диофант (время его жизни точно не известно, приблизительно 200 г. нашей эры) написал книгу *Arithmetica* («Арифметика»), в которой рассматриваются подобные задачи. С этого времени задача нахождения целочисленных или рациональных решений уравнений называется *задачей Диофанта*, а диофантов анализ — важная часть современной теории чисел.

Система задач 1.3.

1. Попробуйте найти другое решение уравнения Пифагора в целых числах.

2. Попробуйте найти решения уравнения Пифагора, в которых гипотенуза на единицу больше, чем больший из двух катетов.

§ 4. Фигурные числа

В теории чисел мы часто встречаемся с квадратами, т. е. такими числами, как

$$3^2 = 9, \quad 7^2 = 49, \quad 10^2 = 100,$$

и аналогично с кубами, т. е. такими числами, как

$$\begin{array}{ccccccc} \cdot & \cdot & \cdot & \cdot & \cdot & 2^3 = 8, & 3^3 = 27, & 5^3 = 125. \end{array}$$

Этот геометрический образ рассматриваемой операции с числами является частью богатого наследства, оставленного древнегреческими мыслителями. Греки предпочитали думать о числах, как о геометрических величинах: произведение $c = a \cdot b$ рассматривалось

Рис. 2

как площадь c прямоугольника со сторонами a и b . Также можно было рассматривать $a \cdot b$ как число точек в прямоугольной таблице с a точками на одной стороне и b точками на другой. Например, $20 = 4 \cdot 5$ есть число точек в прямоугольной таблице на рис. 2.

Любое целое число, которое является произведением двух целых чисел, можно было бы назвать *прямоугольным числом*. Когда две стороны прямоугольника имеют одну и ту же длину, то такое число является *квадратным числом*, или *квадратом*. Некоторые числа нельзя представлять в виде прямоугольных чисел иначе, как тривиальным способом — в виде цепочки точек, лежащих в одном ряду. Например, пять может быть представлено

как прямоугольное число лишь
 • • • • •
 единственным способом, взяв
 одну сторону равной единице,
 а другую — пяти (рис. 3). Та-

Рис. 3.

кие числа греки называли *простыми числами*. Точка, взятая в одном экземпляре, не рассматривалась как число. Число 1 явилось тем кирпичом, из которого строились все остальные числа. *Таким образом, 1 не была для них и не считается сейчас простым числом.*

Можно было бы рассматривать точки, равномерно заполняющие не только прямоугольники и квадраты,

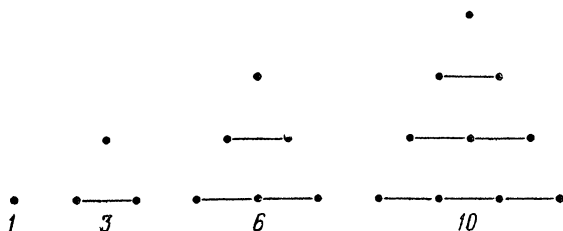


Рис. 4.

но и другие геометрические фигуры. Последовательные *треугольные* числа изображены на рис. 4.

В общем случае n -е треугольное число задается формулой

$$T_n = \frac{1}{2} n (n + 1), \quad n = 1, 2, 3, \dots \quad (1.4.1)$$

У этих чисел масса интересных свойств: например, сумма двух последовательных треугольных чисел является квадратом

$$1 + 3 = 4, \quad 3 + 6 = 9, \quad 6 + 10 = 16 \quad \text{и т. д.} \quad (1.4.2)$$

Обобщением треугольных чисел и квадратов явились многоугольные числа. Метод их получения проиллюстрируем на примере пятиугольных чисел. Для этого рассмотрим рис. 5.

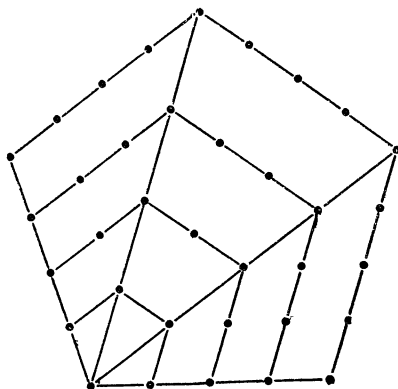


Рис. 5.

Глядя на него, легко найти несколько первых пятиугольных чисел,

$$1, 5, 12, 22, 35. \quad (1.4.3)$$

Можно показать, что n -е пятиугольное число выражается формулой

$$p_n = \frac{1}{2} (3n^2 - n). \quad (1.4.4)$$

Шестиугольные числа, и вообще k -угольные числа, аналогично определяются с помощью правильного k -угольника, и мы не будем больше тратить времени на их обсуждение. Фигурные числа, особенно треугольные, пользовались большой популярностью при изучении чисел в конце эпохи Возрождения, после того как греческая теория чисел проникла в Западную Европу. И сейчас их можно иногда встретить в статьях по теории чисел.

Проводя анализ такого геометрического представления чисел, можно получить несколько простых соотношений. Остановимся лишь на одном примере. Уже давно было известно, что складывая последова-

тельно нечетные числа, мы все время будем получать квадраты, например,

$$1 + 3 = 4, \quad 1 + 3 + 5 = 9, \quad 1 + 3 + 5 + 7 = 16 \quad \text{и т. д.}$$

Чтобы доказать это соотношение, достаточно лишь взглянуть на рис. 6, на котором изображены последовательно вложенные квадраты.

Система задач 1.4.

1. Докажите по индукции общую формулу (1.4.1) для треугольных чисел.

2. Докажите формулу (1.4.4) для пятиугольных чисел.

3. Докажите, что произвольное k -угольное число выражается формулой

$$\frac{1}{2} k (n^2 - n) - n^2 + 2n.$$

§ 5. Магические квадраты

Если вы играли в «шафлборд»*), вы можете вспомнить, что девять квадратов, на которых вы размещаете свои фишки, занумерованы числами от 1 до 9, расположенными так, как на рис. 7. Здесь числа в каждом столбце и в каждой строчке, а также в каждой из диагоналей, дают при сложении одно и то же число 15.

В общем случае *магическим квадратом* является расположение чисел от 1 до n^2 в виде квадрата так, что числа в каждом столбце, строчке и диагонали дают одинаковую сумму s , называемую *магической суммой*.

Пример магического квадрата с $4^2 = 16$ числами изображен на рис. 8. Магическая сумма для него равна 34.

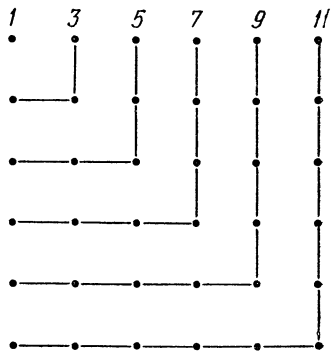


Рис. 6.

*) Игра с передвижением фишек по размеченной доске. (Прим. перев.)

Для каждого числа n существует только одна магическая сумма s , которую легко найти. Так как сумма чисел в каждом столбце равна s , а столбцов — n ; то сумма всех чисел в магическом квадрате равна ns .

2	9	4
7	5	3
6	1	8

Рис. 7.

1	8	15	10
12	13	6	3
14	11	4	5
7	2	9	16

Рис. 8.

Но сумма всех чисел от 1 до n^2 равна

$$1 + 2 + \dots + n^2 = \frac{1}{2} (n^2 + 1) n^2,$$

что следует из формулы для суммы n членов арифметической прогрессии. Так как

$$ns = \frac{1}{2} (n^2 + 1) n^2,$$

то

$$s = \frac{1}{2} n (n^2 + 1). \quad (1.5.1)$$

Таким образом, если число n задано, то число s определено. Магические квадраты могут быть построены для любого числа n , которое больше 2; читатель легко может убедиться, что их не существует для $n = 2$.

Во времена средневековья странные свойства этих квадратов считались волшебными и поэтому магические квадраты служили талисманами, защищающими тех, кто их носил, от многих несчастий. Часто воспроизводится магический квадрат, присутствующий на знаменитой гравюре Альбрехта Дюрера «Меланхолия» (она помещена на фронтисписе нашей книги). Этот квадрат воспроизведен с большим увеличением на рис. 9; при этом мы получили также возможность увидеть, как во времена Дюрера изображались

цифры. Средние числа в последней строке изображают год — 1514, в котором, как мы знаем, была создана эта гравюра. Возможно, что Дюрер, положив в основу именно эти числа, нашел остальные методом проб и ошибок. Можно доказать, что при $n=3$ имеется лишь один магический квадрат, а именно квадрат,

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Рис. 9.

изображенный на рис. 7. Докажем этот факт. Для этого напомним числовой квадрат 3×3 в общем виде

$$x_1 \quad y_1 \quad z_1$$

$$x_2 \quad y_2 \quad z_2$$

$$x_3 \quad y_3 \quad z_3$$

и выясним, какими могут быть эти девять чисел.

Вначале покажем, что центральное число y_2 должно равняться 5. Из формулы (1.5.1) следует, что при $n=3$ магическая сумма s равна 15. Просуммируем теперь числа во второй строке, втором столбце и обеих диагоналях. В эту сумму каждое число, кроме числа y_2 , входит по одному разу; число y_2 входит четыре раза, так как оно содержится в каждой из четырех

сумм. Поэтому, так как каждая сумма равна s , то

$$4s = 4 \times 15 = 60 =$$

$$\begin{aligned} &= x_2 + y_2 + z_2 + y_1 + y_2 + y_3 + x_1 + y_2 + \\ &\quad + z_3 + z_1 + y_2 + x_3 = 3y_2 + x_1 + x_2 + \\ &\quad + x_3 + y_1 + y_2 + y_3 + z_1 + z_2 + z_3 = \\ &= 3y_2 + 1 + 2 + \dots + 9 = 3y_2 + 45. \end{aligned}$$

Следовательно,

$$3y_2 = 60 - 45 = 15 \quad \text{и} \quad y_2 = 5.$$

В таблице

x_1	y_1	z_1
x_2	5	z_2
x_3	y_3	z_3

число 9 не может стоять в углу, так как, если, например, $x_1 = 9$, то $z_3 = 1$ (потому что $s = 15$), т. е. мы получили бы таблицу

9	y_1	z_1
x_2	5	z_2
x_3	y_3	1

Каждое из четырех чисел y_1, z_1, x_2, x_3 должно быть меньше шести, так как $y_1 + z_1 = x_2 + x_3 = 6$. Но у нас осталось лишь три числа, меньших шести, а именно: 2, 3 и 4. Таким образом, получилось противоречие. Отсюда мы делаем вывод, что число 9 должно находиться в середине строки или столбца, поэтому наш квадрат может быть записан так:

x_1	9	z_1
x_2	5	z_2
x_3	1	z_3

Число 7 не может быть в одной и той же строке с числом 9, так как тогда сумма чисел в этой строке была бы больше пятнадцати; точно так же число 7 не может быть в одной и той же строке с числом 1, так как тогда оставшееся в этой строке число должно было бы быть также семеркой. Таким образом, 7 не может находиться в углу, и мы можем считать, что наш квадрат имеет следующий вид:

x_1	9	z_1
7	5	3
x_3	1	z_3

Числа, находящиеся в одной строке с числом 9 — это 2 и 4, так как иначе сумма в этой строке была бы больше пятнадцати. Далее, число 2 должно быть в том же столбце, что и число 7, так как если бы там стояло 4, то третье число в этом столбце было бы тоже 4. Используя это наблюдение, мы можем определить место каждого из двух оставшихся чисел 6 и 8, в результате получаем магический квадрат, изображенный на рис. 7.

Для больших значений n можно построить великое множество магических квадратов. В XVI и XVII веках, и даже позже, составление магических квадратов столь же процветало, как и составление кроссвордов в наши дни. Бенджамин Франклин *) был страстным любителем магических квадратов. Он позже признавался, что, будучи служащим Законодательного Собрания штата Пенсильвания, он скрашивал скучные часы на службе составлением причудливых магических квадратов и даже магических кругов, в которых числа стоят на переплетающихся окружностях, причем сумма чисел на каждой из окружностей одна и та же. Следующий эпизод взят нами из Собрания сочинений Бенджамина Франклина **).

О магических квадратах Б. Франклина стало известно, когда один из его старых друзей, Логан, показал ему несколько книг о магических квадратах, заметив при этом, что не верит в то, что кто-либо из англичан мог бы сделать что-либо замечательное в этой области.

«Логан показал мне в одной из этих книг несколько необычных и довольно любопытных случаев, но ни один из них не мог сравниться с теми, которые, как я помню, были сделаны мною. Он попросил меня показать их. И в следующее свое посещение я принес ему квадрат 8×8 , который я нашел среди своих старых бумаг и который я предлагаю вам с описанием его свойств» (рис. 10).

Б. Франклин упоминает только некоторые свойства своего квадрата. Мы предлагаем читателю найти

*) Бенджамин Франклин (1706—1790) — выдающийся американский общественный деятель, дипломат и ученый. (Прим. перев.)

**) The Papers of Benjamin Franklin, Yale University Press, т. 4, с. 392—402.

и другие его свойства. Например, очевидно, что s равняется 260, а сумма чисел в каждой половине любой строки и в каждой половине любого столбца равняется 130, что составляет половину от 260. Четыре числа, стоящие в углах, в сумме с четырьмя числами, стоящими в центре квадрата, дают 260; сумма чисел по наклонному ряду, идущему от числа 16 вправо — вверх до числа 10, а далее по наклонному ряду, идущему от числа 23 вправо — вниз до числа 17 равна

260. То же самое верно для каждого ряда из восьми чисел, параллельного описанному выше.

«Потом Логан показал мне старую книгу по арифметике, изданную в формате кварто*) и написанную, я думаю, неким Штифелем (Михаил Штифель, «*Arithmetica integra*», Нюрнберг, 1544). В этой книге был помещен квадрат 16×16 , в который, по его мнению, был вложен колоссаль-

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

Рис. 10.

ный труд. Но если я не ошибаюсь, он имел лишь обычное свойство, т. е. обладал постоянной суммой, равной 2056 в каждом ряду: горизонтальном, вертикальном и диагональном.

Не желая уступить Штифелю даже в размерах квадрата, я, вернувшись домой, в тот же вечер составил квадрат 16×16 , который помимо всех свойств моего квадрата 8×8 , т. е. наличия постоянной суммы 2056 во всех аналогичных рядах и диагоналях, имел еще одно дополнительное свойство. Если вырезать из листа бумаги квадрат 4×4 и уложить этот лист на большой квадрат так, чтобы 16 квадратиков большего квадрата попали в эту прорезь, то сумма 16 чисел, появившихся в этой прорези, куда бы мы ее ни положили, на большом квадрате будет одна и та же, и равна тому же самому числу 2056».

*) Формат кварто — формат в $1/4$ долю листа, т. е. $450 \text{ мм} \times 300 \text{ мм}$. (Прим. перев.)

Магический квадрат Б. Франклина перед вами (рис. 11) и вы можете сами проверить его замечательные свойства.

Б. Франклин по праву гордился своим творением, что видно из продолжения его письма: «На следующее утро я послал этот квадрат нашему другу, который через несколько дней вернул его в ответном

200	217	232	249	8	25	40	57	72	89	104	121	136	153	168	185
58	39	26	7	250	231	218	199	186	167	154	135	122	103	90	71
198	219	230	251	6	27	38	59	70	91	102	123	134	155	166	187
60	37	28	5	252	229	220	197	188	165	156	133	124	101	92	69
201	216	233	248	9	24	41	56	73	88	105	120	137	152	169	184
55	42	23	10	247	234	215	202	183	170	151	138	119	106	87	74
203	214	235	246	11	22	43	54	75	86	107	118	139	150	171	182
53	44	21	12	245	236	213	204	181	172	149	140	117	108	85	76
205	212	237	244	13	20	45	52	77	84	109	116	141	148	173	180
51	46	19	14	243	238	211	206	179	174	147	142	115	110	83	78
207	210	239	242	15	18	47	50	79	82	111	114	143	146	175	178
49	48	17	16	241	240	209	208	177	176	145	144	113	112	81	80
196	221	228	253	4	29	36	61	68	93	100	125	132	157	164	189
62	35	30	3	254	227	222	195	190	163	158	131	126	99	94	67
194	223	226	255	2	31	34	63	66	95	98	127	130	159	162	191
64	33	32	1	256	225	224	193	192	161	160	129	128	97	96	65

Рис. 11.

письме со следующими словами: „Я возвращаю тебе твой удивительный, а может быть, самый изумительный магический квадрат, в котором...“, но этот комплимент слишком экстравагантен, и поэтому ради него, а также ради самого себя, мне не следует его повторять. К тому же это и необязательно, так как я не сомневаюсь, что вы охотно согласитесь, что этот квадрат 16×16 является самым магически-магическим из всех магических квадратов, составленных

когда-либо каким-либо магом». Более подробные сведения о построении магических квадратов можно найти в книгах: Е. Я. Гуревич. Тайна древнего талисмана. — М.: Наука, 1969 и И. М. Постников. Магические квадраты. — М.: Наука, 1964.

Система задач 1.5.

1. Мог ли Дюрер использовать вместо своего квадрата, изображенного на рис. 9, какие-либо дру-

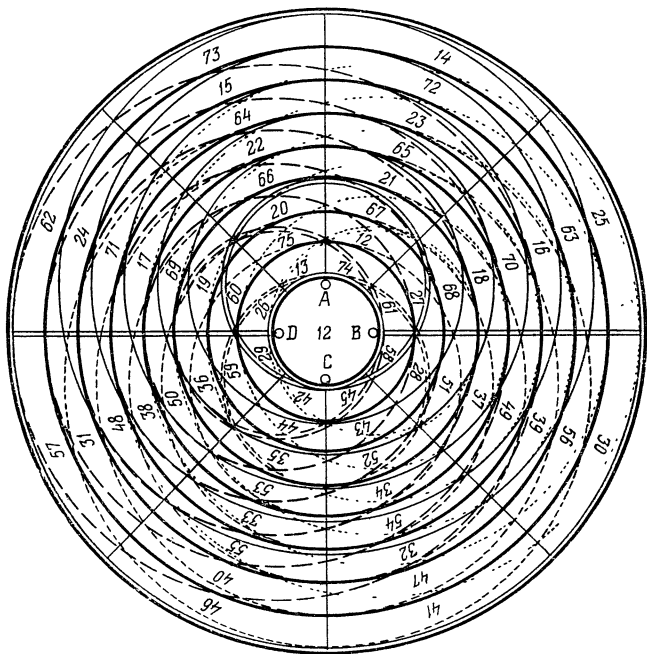


Рис. 12. Репродукция магического круга Франклина. Оригинал, выполненный в цвете, был продан частному коллекционеру на аукционе в Нью-Йорке.

гие квадраты, в которых тот же год фигурировал таким же образом?

2. Дюрер прожил до 1528 г. Смог ли бы он датировать какую-нибудь из своих более поздних картин таким же способом?

3. Изучите некоторые свойства магического круга Б. Франклина (рис. 12).

ПРОСТЫЕ ЧИСЛА

§ 1. Простые и составные числа

‘Должно быть, одним из первых свойств чисел, открытых человеком, было то, что некоторые из них могут быть разложены на два или более множителя, например,

$$6 = 2 \cdot 3, \quad 9 = 3 \cdot 3, \quad 30 = 2 \cdot 15 = 3 \cdot 10,$$

в то время как другие, например,

$$3, \quad 7, \quad 13, \quad 37,$$

не могут быть разложены на множители подобным образом. Давайте вспомним, что вообще, когда число

$$c = a \cdot b \tag{2.1.1}$$

является произведением двух чисел a и b , то мы называем a и b *множителями* или *делителями* числа c . Каждое число имеет *тривиальное разложение* на множители

$$c = 1 \cdot c = c \cdot 1. \tag{2.1.2}$$

Соответственно мы называем числа 1 и c *тривиальными делителями* числа c .

Любое число $c > 1$, у которого существует нетривиальное разложение на множители, называется *составным*. Если число c имеет только тривиальное разложение на множители (2.1.2), то оно называется *простым*. Среди первых 100 чисел простыми являются следующие 25 чисел:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \\ 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Все остальные числа, кроме 1 , являются составными. Мы можем сформулировать следующее утверждение:

Теорема 2.1.1. *Любое целое число $c > 1$ является либо простым, либо имеет простой множитель.*

Доказательство. Если c не является простым числом, то у него есть наименьший нетривиальный множитель p . Тогда p — простое число, так как если бы p было составным, то число c имело бы еще меньший множитель.

Теперь мы подошли к нашей первой важной задаче в теории чисел: как определить, является ли произвольное число простым или нет, и в случае, если оно составное, то как найти какой-либо его нетривиальный делитель?

Первое, что может прийти в голову, — это попытаться разделить данное число c на все числа, меньшие его. Но надо признать, что этот способ мало удовлетворителен. Согласно теореме 2.1.1 достаточно делить на все простые числа, меньшие c . Но мы можем значительно упростить задачу, заметив, что при разложении на множители (2.1.1) оба множителя a и b не могут быть больше, чем \sqrt{c} , так как в противном случае мы получили бы

$$a \cdot b > \sqrt{c} \cdot \sqrt{c} = c,$$

что невозможно. Таким образом, чтобы узнать, имеет ли число c делитель, достаточно проверить, делится ли число c на простые числа, не превосходящие \sqrt{c} .

Пример 1. Если $c = 91$, то $\sqrt{c} = 9, \dots$; проверив простые числа 2, 3, 5, 7, находим, что $91 = 7 \cdot 13$.

Пример 2. Если $c = 1973$, то находим, что $\sqrt{c} = 44, \dots$. Так как ни одно из простых чисел до 43 не делит c , то это число является простым.

Очевидно, что для больших чисел этот метод может быть очень трудоемким. Однако здесь, как и при многих других вычислениях в теории чисел, можно использовать современные методы. Довольно просто запрограммировать на ЭВМ деление данного числа c на все целые числа до \sqrt{c} и печатание тех из них, которые не имеют остатка, т. е. тех, которые делят c .

Другим очень простым методом является применение таблиц простых чисел, т. е. использование простых чисел уже найденных другими. За последние 200 лет было составлено и издано много таблиц простых чисел. Наиболее обширной из них является таб-

лица Д. Х. Лемера, содержащая все простые числа до 10 000 000. Наша таблица 1 содержит все простые числа до 1000.

Таблица 1

Простые числа среди первой тысячи чисел

2,	3,	5,	7,	11,	13,	17,	19,	23,	29,	31,	37,
41,	43,	47,	53,	59,	61,	67,	71,	73,	79,	83,	89,
97,	101,	103,	107,	109,	113,	127,	131,	137,	139,	149,	151,
157,	163,	167,	173,	179,	181,	191,	193,	197,	199,	211,	223,
227,	229,	233,	239,	241,	251,	257,	263,	269,	271,	277,	281,
283,	293,	307,	311,	313,	317,	331,	337,	347,	349,	353,	359,
367,	373,	379,	383,	389,	397,	401,	409,	419,	421,	431,	433,
439,	443,	449,	457,	461,	463,	467,	479,	487,	491,	499,	503,
509,	521,	523,	541,	547,	557,	563,	569,	571,	577,	587,	593,
599,	601,	607,	613,	617,	619,	631,	641,	643,	647,	653,	659,
661,	673,	677,	683,	691,	701,	709,	719,	727,	733,	739,	743,
751,	757,	761,	769,	773,	787,	797,	809,	811,	821,	823,	827,
829,	839,	853,	857,	859,	863,	877,	881,	883,	887,	907,	911,
919,	929,	937,	941,	947,	953,	967,	971,	977,	983,	991,	997,

Некоторые энтузиасты-вычислители уже подготовили таблицы простых чисел, превосходящих 10 000 000. Но, по-видимому, не имеет большого смысла идти на значительные затраты и усилия, чтобы опубликовать эти таблицы. Лишь в очень редких случаях математику, даже специалисту в теории чисел, приходится решать вопрос, о том, является ли какое-то большое число простым. Кроме того, большие числа, о которых математик хочет узнать, являются они составными или простыми, не берутся им произвольно. Числа, которые он хочет исследовать, обычно появляются в специальных математических задачах, и, таким образом, эти числа имеют очень специфическую форму.

Система задач 2.1.

1. Какие из следующих чисел являются простыми:
а) год вашего рождения; б) текущий год; в) номер вашего дома.

2. Найдите простое число, следующее за простым числом 1973.

3. Заметим, что числа от 90 до 96 включительно являются семью последовательными составными числами; найдите девять последовательных составных чисел.

§ 2. Простые числа Мерсенна

В течение нескольких столетий шла погоня за простыми числами. Многие математики боролись за честь стать открывателем самого большого из известных простых чисел. Разумеется, можно было бы выбрать несколько очень больших чисел, не имеющих таких очевидных делителей, как 2, 3, 5, 7, и проверить, являются ли они простыми числами. Этот способ, как мы вскоре убедимся, не очень эффективен. Теперь эта погоня утихла, она идет только в одном направлении, оказавшемся удачным.

Простые числа Мерсенна являются простыми числами специального вида

$$M_p = 2^p - 1, \quad (2.2.1)$$

где p — другое простое число. Эти числа вошли в математику давно, они появляются еще в евклидовых размышлениях о совершенных числах, которые мы рассмотрим позже. Свое название они получили в честь французского монаха Мерена Мерсенна (1588—1648), который много занимался проблемой совершенных чисел.

Если начать вычислять числа (2.2.1) для различных простых чисел p , то видно, что не все они оказываются простыми. Например,

$$M_2 = 2^2 - 1 = 3 = \text{простое},$$

$$M_3 = 2^3 - 1 = 7 = \text{простое},$$

$$M_5 = 2^5 - 1 = 31 = \text{простое},$$

$$M_7 = 2^7 - 1 = 127 = \text{простое},$$

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89.$$

Общий способ нахождения больших простых чисел Мерсенна состоит в проверке всех чисел M_p для различных простых чисел p .

Эти числа очень быстро увеличиваются и столь же быстро увеличиваются затраты труда на их нахождение. То, что с этой работой все-таки можно спра-

виться уже для довольно больших чисел, объясняется существованием эффективных способов выяснения простоты для чисел такого вида.

В исследовании чисел Мерсенна можно выделить раннюю стадию, достигшую своей кульминации в 1750 году, когда Леонард Эйлер *) установил, что число M_{31} является простым. К этому времени было найдено восемь простых чисел Мерсенна, соответствующих значениям

$$\begin{aligned} p=2, & \quad p=3, & \quad p=5, & \quad p=7, \\ p=13, & \quad p=17, & \quad p=19, & \quad p=31. \end{aligned}$$

Эйлерово число M_{31} оставалось самым большим из известных простых чисел более ста лет. В 1876 году французский математик Лукас установил, что огромное число

$$M_{127} = 170141183460469231731687303715884105727$$

является простым числом. Ну и число! С 39 цифрами. Простые числа Мерсенна, меньшие этого числа, задаются значениями p , указанными выше, а также значениями

$$p=61, \quad p=89, \quad p=107.$$

Эти 12 простых чисел Мерсенна были вычислены с помощью только карандаша и бумаги, а для вычисления следующих уже использовались механические настольные счетные машины. Появление вычислительных машин с электрическим приводом позволило продолжить поиски, доведя их до $p=257$. Однако результаты были неутешительными, среди них не оказалось новых простых чисел Мерсенна.

Затем задача была переложена на плечи ЭВМ. Создание все более высокопроизводительных ЭВМ дало возможность продолжить поиск новых простых чисел Мерсенна. Д. Х. Лемер установил, что значения

$$\begin{aligned} p=521, & \quad p=607, & \quad p=1279, \\ p=2203, & \quad p=2281 \end{aligned}$$

*) Леонард Эйлер (1707—1783) — выдающийся математик, родившийся в Швейцарии, большую часть жизни провел в России, являясь членом Петербургской Академии наук. (Прим. перев.)

дают простые числа Мерсенна. Дальнейшие поиски также увенчались успехом. Ризель (1958) показал, что

$$p = 3217,$$

дает простое число Мерсенна, а Гурвиц (1962) нашел еще два таких значения:

$$p = 4253, \quad p = 4423.$$

Огромного успеха добился Гиллельс (1964), который нашел простые числа Мерсенна, соответствующие значениям

$$p = 9689, \quad p = 9941, \quad p = 11213.$$

Итак, общий урожай составил 23 простых числа Мерсенна, и, так как мощности ЭВМ продолжают увеличиваться, мы надеемся на дальнейший успех. Простое число Лукаса M_{127} , как мы уже упоминали, имеет 39 цифр. Даже вычисление самого большого из известных простых чисел, числа M_{11213} , является довольно сложной задачей и, по-видимому, нет смысла воспроизводить здесь это число. Если же мы захотим узнать, сколько цифр содержит это число, то мы можем сделать это, не вычисляя самого числа.

Вместо нахождения количества цифр числа $M_p = 2^p - 1$ рассмотрим эту задачу для числа

$$M_p + 1 = 2^p.$$

Эти два числа имеют одинаковое количество цифр, так как если бы число $M_p + 1$ имело на одну цифру больше, то оно должно было бы оканчиваться на 0. Но это невозможно ни для какой степени числа 2, что видно из ряда

$$2, 4, 8, 16, 32, 64, 128, 256, \dots,$$

в котором последняя цифра в каждом числе может быть только одним из чисел

$$2, 4, 8, 6.$$

Чтобы найти количество цифр числа 2^p , вспомним, что $\lg 2^p = p \lg 2$. Из таблиц находим, что $\lg 2$ приближенно равняется 0,30103, откуда

$$\lg 2^p = p \lg 2 = p \cdot 0,30103.$$

Для $p = 11213$ получаем

$$\lg 2^{11213} = 3375,449 \dots,$$

и так как характеристика этого числа равна 3375, то мы приходим к выводу, что число 2^p имеет 3376 цифр. Итак, мы можем сказать следующее.

Самое большое известное в настоящее время простое число имеет 3376 цифр. (Здесь слова «в настоящее время» имеют существенное значение.) Это число было найдено на ЭВМ Иллинойского университета (США). Математический факультет этого университета был так горд своим достижением, что изобразил это число на своем почтовом штампе, таким образом воспроизводя его на каждом отсылаемом письме, для всеобщего восхищения.

§ 3. Простые числа Ферма

Существует также еще один тип простых чисел с большой и интересной историей. Они были впервые введены французским юристом Пьером Ферма́ (1601—1665), который прославился своими выдающимися математическими работами. Первыми пятью простыми числами Ферма являются

$$\begin{aligned} F_0 &= 2^0 + 1 = 3, & F_1 &= 2^1 + 1 = 5, \\ F_2 &= 2^2 + 1 = 17, & F_3 &= 2^3 + 1 = 257, \\ F_4 &= 2^4 + 1 = 65\,537. \end{aligned}$$

В соответствии с этой последовательностью общая формула для простых чисел Ферма должна иметь вид

$$F_n = 2^{2^n} + 1. \quad (2.3.1)$$

Ферма был абсолютно уверен, что все числа этого вида являются простыми, хотя он не проводил вычислений других чисел, кроме указанных пяти. Однако это предположение было сдано в архив неоправдавшихся математических гипотез после того, как Леонард Эйлер сделал еще один шаг и показал, что следующее число Ферма

$$F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$$

не является простым, что и показывает приведенная запись. Возможно, что этим история чисел Ферма

была бы закончена, если бы числа Ферма не появились в совсем другой задаче, задаче построения правильных многоугольников при помощи циркуля и линейки.

Правильным многоугольником называется многоугольник, вершины которого лежат на некоторой окружности на одинаковых расстояниях друг от друга (рис. 13). Если у правильного многоугольника n вершин, то мы называем его *правильным n -угольником*. Если мы проведем n радиусов, соединяющих центр окружности с вершинами, то получим n центральных углов величиной

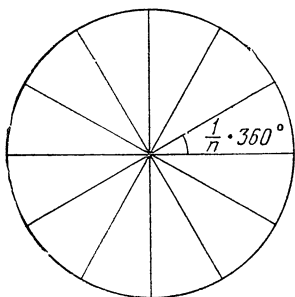


Рис 13.

$$\frac{1}{n} \cdot 360^\circ$$

каждый. Если можно построить угол, имеющий эту величину, то можно построить и этот n -угольник.

Древние греки очень хотели найти методы построения правильных многоугольников с помощью циркуля и линейки. Разумеется, они умели строить простейшие из них — равносторонний треугольник и квадрат. С помощью повторного деления пополам центрального угла они могли также построить правильные многоугольники с

4, 8, 16, 32, ...

3, 6, 12, 24, ...

вершинами. Кроме того, они умели строить правильный пятиугольник, и следовательно, также правильные многоугольники с

5, 10, 20, 40, ...

вершинами. Был также получен еще один тип правильного многоугольника. Центральный угол в правильном 15-угольнике равен

$$\frac{1}{15} \cdot 360^\circ = 24^\circ,$$

и он может быть получен с помощью угла в 72° , соответствующего правильному пятиугольнику, и угла в

120°, соответствующего правильному треугольнику, если удвоить первый угол и вычесть из него второй. Следовательно, мы можем построить правильные многоугольники с 15, 30, 60, 120, ... сторонами.

В таком состоянии проблема оставалась до 1801 года, когда вышла работа по теории чисел молодого немецкого математика К. Ф. Гаусса (1777—1855) «Арифметические исследования». Она открыла новую эпоху в математике. Гаусс превзошел греческих геометров не только в том, что указал метод построения циркулем и линейкой правильного 17-угольника, но и пошел гораздо дальше. Для всех чисел n он определил, какие n -угольники могут быть построены таким образом, а какие нет. Сейчас мы опишем результаты, полученные Гауссом.

Выше мы отмечали, что из правильного n -угольника можно получить правильный $2n$ -угольник, деля каждый центральный угол пополам. С другой стороны, из $2n$ -угольника можно получить n -угольник, используя лишь каждую вторую вершину. Это показывает, что достаточно провести поиск правильных многоугольников, которые могут быть построены с помощью циркуля и линейки, только среди многоугольников с нечетным числом вершин. Гаусс доказал, что *правильный n -угольник с нечетным числом вершин может быть построен с помощью циркуля и линейки тогда, и только тогда, если число n является простым числом Ферма или произведением нескольких различных простых чисел Ферма.*

Что это нам дает для небольших значений n ? Очевидно, что 3-угольник и 5-угольник могут быть построены, в то время как 7-угольник не может, так как 7 не является простым числом Ферма. Не может быть построен и 9-угольник, так как $9 = 3 \cdot 3$ является произведением двух равных простых чисел Ферма. Для $n = 11$ и $n = 13$ многоугольники не могут быть построены, но можно построить для $n = 15 = 3 \cdot 5$ и $n = 17$.

Открытие Гаусса, естественно, возродило интерес к числам Ферма (2.3.1). За последнее столетие были предприняты поистине героические поиски, вручную, без помощи машин, новых простых чисел Ферма. В настоящее время эти вычисления продолжают со все возрастающей скоростью с помощью ЭВМ.

Однако до сих пор результаты были отрицательными. Ни одного нового простого числа Ферма не было найдено и сейчас многие математики склонны считать, что их больше нет.

Система задач 2.3.

1. Найдите все нечетные числа $n < 100$, для которых можно построить правильный n -угольник.

2. Как построить правильный 51-угольник, имея правильный 17-угольник?

3. Если не существует простых чисел Ферма, кроме выше указанных пяти, то сколько существует правильных n -угольников (n нечетно), которые могут быть построены циркулем и линейкой? Каково то наибольшее нечетное n , для которого может быть построен правильный n -угольник?

§ 4. Решето Эратосфена

Как мы уже говорили, существуют таблицы простых чисел, простирающиеся до очень больших чисел. Как можно было бы подступиться к составлению такой таблицы? Эта задача была, в известном смысле, решена (около 200 г. до н. э.) Эратосфеном, математиком из Александрии. Его схема состоит в следующем: напишем последовательность всех целых чисел от 1 до числа, которым мы хотим закончить таблицу:

$$\begin{array}{cccccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ & & & \frac{2}{2} & & \frac{2}{2} & & \frac{2}{2} & \frac{3}{3} & \frac{2}{2} & & \frac{2}{2} & & \frac{2}{2} & \frac{3}{3} \end{array}$$

Начнем с простого числа 2. Будем выбрасывать каждое второе число, начиная с 2 (кроме самого числа 2), т. е. четные числа 4, 6, 8, 10 и т. д., подчеркивая каждое из них. После этой операции первым неподчеркнутым числом будет число 3. Оно простое, так как не делится на 2. Оставив число 3 неподчеркнутым, будем подчеркивать каждое третье число после него, т. е. числа 6, 9, 12, 15, ... ; некоторые из них уже были подчеркнуты, поскольку они являются четными. На следующем шаге первым неподчеркнутым числом окажется число 5; оно простое, так как не делится ни на 2, ни на 3. Оставим число 5 неподчеркнутым, но подчеркнем каждое пятое число после

него, т. е. числа 10, 15, 20, 25, ... ; как и раньше, часть из них уже оказалась подчеркнутой. Теперь наименьшим неподчеркнутым числом окажется число 7. Оно простое, так как не делится ни на одно из меньших его простых чисел 2, 3, 5. Повторяя этот процесс, мы в конце концов получим последовательность неподчеркнутых чисел; все они (кроме числа 1) являются простыми.

Этот метод отсеивания чисел известен как «решето Эратосфена». Любая таблица простых чисел создается по этому принципу решета. В действительности, можно продвинуться гораздо дальше по ряду простых чисел, если использовать для их хранения память ЭВМ. Подобным образом, в Научно-исследовательской лаборатории Лос-Аламоса были получены все простые числа до 100 000 000.

Небольшое изменение метода решета позволит нам получить большую информацию. Предположим, что всякий раз, впервые подчеркивая числа, мы будем подписывать под ним простое число, с помощью которого оно отсеивается. Тогда 15 и 35 были бы записаны как

$$\frac{15}{3}, \quad \frac{35}{5}$$

и т. д., как это показано на последовательности, выписанной выше. Таким образом, мы не только указали простые числа, но и для каждого составного числа привели наименьшее простое число, являющееся его делителем. Такой список чисел называется таблицей делителей. Таблица делителей является более сложной, чем таблица простых чисел. Чтобы немного упростить ее, обычно из нее исключают те составные числа, у которых простые делители малы, например, 2, 3, 5, 7. Самая большая такая таблица была вычислена на ЭВМ Д. Х. Лемером и содержит все числа, вплоть до 10 000 000.

Как мы видели, решето Эратосфена может быть использовано для построения таблиц простых чисел и таблиц делителей. Однако оно может быть использовано и для теоретических исследований. Многие важные результаты в современной теории чисел были получены методом решета. Приведем результат, известный еще Евклиду:

Существует бесконечное число простых чисел.

Доказательство. Предположим, что существует только k простых чисел:

$$2, 3, 5, \dots, p_k.$$

Тогда в решете не оказалось бы неподчеркнутых чисел, больших, чем p_k . Но это невозможно, так как произведение этих простых чисел

$$p = 2 \cdot 3 \cdot 5 \dots p_k$$

будет отсеиваться k раз, по разу для каждого простого числа, поэтому следующее число $p + 1$ не может быть подчеркнуто ни для одного из них.

Система задач 2.4.

1. Составьте таблицы простых чисел для каждой из сотен: 1—100, 101—200, ..., 901—1000.

2. Попытайтесь определить количество простых чисел в диапазоне 10001—10100.

ДЕЛИТЕЛИ ЧИСЕЛ

§ 1. Основная теорема о разложении на множители

Любое составное число c может быть записано в виде произведения $c = a \cdot b$, причем ни один из делителей не равен 1 и каждый из них меньше, чем c ; например,

$$72 = 8 \cdot 9, \quad 150 = 10 \cdot 15.$$

При разложении числа c на множители один из них, и даже оба (a и b) могут оказаться составными. Если a — составное, то разложение на множители можно продолжить:

$$a = a_1 \cdot a_2, \quad c = a_1 \cdot a_2 \cdot b.$$

Примерами этого могут служить рассмотренные выше числа

$$72 = 2 \cdot 4 \cdot 9, \quad 150 = 2 \cdot 5 \cdot 15.$$

Этот процесс разложения на множители можно продолжить до тех пор, пока он не закончится; это должно произойти, так как делители становятся все меньше и меньше, но не могут стать единицей. Когда ни один из делителей нельзя уже будет разложить на множители, то все делители будут простыми числами. Таким образом мы показали, что

Каждое целое число, большее 1, является простым числом или произведением простых чисел.

Последовательное разложение числа на множители может быть выполнено многими способами. При этом можно использовать таблицу делителей. Сначала найдем наименьшее простое число p_1 , делящее число c , так что $c = p_1 \cdot c_1$. Если c_1 — составное число,

то по таблице делителей найдем наименьшее простое число p_2 , делящее c_1 , так что

$$c_1 = p_2 \cdot c_2, \quad c = p_1 \cdot p_2 \cdot c_2.$$

Затем найдем наименьший простой делитель числа c_2 и т. д.

Но главное здесь то, что независимо от способа разложения числа на простые множители результат всегда будет одним и тем же, различаясь лишь порядком их записи, т. е. любые два разложения числа на простые множители содержат одни и те же простые числа; при этом каждое простое число содержится одинаковое число раз в обоих разложениях. Этот результат мы можем кратко выразить следующим образом:

разложение числа на простые множители единственно.

Возможно, что вы так часто слышали об этой так называемой «основной теореме арифметики» и пользовались ею, что она представляется вам очевидной, но это совсем не так. Эта теорема может быть доказана несколькими различными способами, однако ни один из них не тривиален. Здесь мы приведем доказательство, используя способ «от противного», который часто называют его латинским названием *reductio ad absurdum* (приведением к абсурду). Этот способ заключается в следующем: предположив ложность теоремы, которую нужно доказать, показывают, что это предположение приводит к противоречию.

Доказательство. Предположим, что наша теорема о единственности разложения на множители неверна. Тогда должны существовать числа, имеющие по крайней мере два различных разложения на простые множители. Выберем из них наименьшее и обозначим его через c_0 . Для небольших чисел, скажем, меньших 10, истинность теоремы можно установить прямой проверкой. Число c_0 имеет наименьший простой множитель p_0 , и мы можем записать:

$$c_0 = p_0 \cdot d_0.$$

Так как $d_0 < c_0$, то число d_0 единственным образом раскладывается на простые множители. Отсюда сле-

дует, что разложение числа c_0 на простые множители, содержащее число p_0 , единственно.

А так как, по предположению, имеется по крайней мере два разложения числа c_0 на простые множители, то должно быть разложение, не содержащее число p_0 . Наименьшее простое число в этом разложении мы обозначим через p_1 и запишем

$$c_0 = p_1 \cdot d_1. \quad (3.1.1)$$

Так как $p_1 > p_0$, то $d_1 < d_0$ и, следовательно, $p_0 d_1 < c_0$. Рассмотрим число

$$c'_0 = c_0 - p_0 d_1 = (p_1 - p_0) d_1. \quad (3.1.2)$$

Так как оно меньше, чем число c_0 , то оно должно раскладываться на простые множители единственным способом; при этом простые множители числа c'_0 состоят из простых множителей чисел $p_1 - p_0$ и d_1 . Так как число c_0 делится на p_0 , то из выражения (3.1.2) следует, что число c'_0 также делится на p_0 . Следовательно, p_0 должно быть делителем либо числа d_1 , либо $p_1 - p_0$. Но любой простой делитель числа d_1 больше, чем p_0 , так как p_1 — наименьшее простое число в разложении (3.1.1). Таким образом, остается единственная возможность: p_0 должно быть делителем числа $p_1 - p_0$ и, следовательно, оно делит p_1 . Итак, мы пришли к противоречию, потому что p_1 является простым числом и не может делиться на другое простое число p_0 .

Выше мы отмечали, что единственность разложения числа на простые множители совсем не очевидна. В действительности, существуют «арифметики», в которых аналогичная теорема не выполняется. Простейшим примером такой арифметики может служить арифметика четных чисел

$$2, 4, 6, 8, 10, 12, \dots$$

Некоторые из них могут быть разложены на два четных множителя, а другие — нет; последние мы называем *четно-простыми числами*. Это числа, которые делятся на 2, но не делятся на 4:

$$2, 6, 10, 14, 18, \dots$$

Очевидно, что каждое четное число либо является четно-простым, либо записывается в виде произведения

четно-простых чисел. Но такое разложение на четно-простые числа не всегда будет единственным. Например, число 420 может быть разложено на четно-простые числа различными способами:

$$420 = 6 \cdot 70 = 10 \cdot 42 = 14 \cdot 30.$$

Система задач 3.1.

1. Найдите разложение на простые множители каждого из чисел 120, 365, 1970.

2. Прodelайте то же самое для чисел, указанных в задаче 1 системы задач 2.1 (стр. 25).

3. Запишите все разложения числа 360 на четно-простые числа.

4. В каких случаях четные числа обладают единственным разложением на четно-простые множители?

§ 2. Делители

Разложим на множители какое-нибудь число, скажем, 3600. Это разложение

$$3600 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5$$

может быть записано как

$$3600 = 2^4 \cdot 3^2 \cdot 5^2.$$

Вообще при разложении числа n на множители аналогично можно собирать одинаковые простые множители в виде степеней и записывать

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}, \quad (3.2.1)$$

где p_1, p_2, \dots, p_r — различные простые множители числа n , причем число p_1 входит α_1 раз, p_2 входит α_2 раз и т. д.

Если мы знаем вид (3.2.1) для числа, то мы сможем тотчас же ответить на некоторые вопросы об этом числе.

Например, если мы захотим, то можем узнать, какие числа делят число n . Возьмем для примера рассмотренное выше число 3600. Предположим, что число d является одним из его делителей, т. е.

$$3600 = d \cdot d_1.$$

Приведенное разложение на простые множители показывает, что единственными числами среди множи-

телей числа d будут лишь 2, 3, 5. Кроме того, число 2 может содержаться не более 4 раз, а числа 3 и 5 не более, чем по 2 раза каждое. Итак, мы видим, что возможными делителями числа 3600 будут числа вида

$$d = 2^{\delta_1} \cdot 3^{\delta_2} \cdot 5^{\delta_3},$$

при этом показатели степени могут принимать значения:

$$\delta_1 = 0, 1, 2, 3, 4; \quad \delta_2 = 0, 1, 2;$$

$$\delta_3 = 0, 1, 2.$$

Так как эти значения могут сочетаться всеми возможными способами, то число делителей равно

$$(4 + 1)(2 + 1)(2 + 1) = 5 \cdot 3 \cdot 3 = 45.$$

Для любого числа n , разложение которого на простые множители дается формулой (3.2.1), положение точно такое же. Если число d является делителем числа n , т. е.

$$n = d \cdot d_1,$$

то единственными простыми числами, на которые может делиться число d , будут только те, которые делят число n , а именно: p_1, \dots, p_r . Таким образом, мы можем записать разложение числа d на простые множители в виде

$$d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_r^{\delta_r}. \quad (3.2.2)$$

Простое число p_1 может содержаться не более α_1 раз, как и в самом числе n ; аналогично — для p_2 и других простых чисел. Это значение для числа δ_1 мы можем выбрать $\alpha_1 + 1$ способом:

$$\delta_1 = 0, 1, \dots, \alpha_1;$$

аналогично и для других простых чисел. Так как каждое из $\alpha_1 + 1$ значений, которые может принимать число δ_1 , может сочетаться с любым из $\alpha_2 + 1$ возможных значений числа δ_2 и т. д., то мы видим, что общее число делителей числа n задается формулой

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1). \quad (3.2.3)$$

Система задач 3.2.

1. Сколько делителей имеет простое число? Сколько делителей имеет степень простого числа p^α ?

2. Найдите количество делителей у следующих чисел: 60, 366, 1970, вашего почтового индекса.

3. Какое натуральное число (или числа), не превосходящее 100, имеет наибольшее количество делителей?

§ 3. Несколько задач о делителях

Существует единственное число $n = 1$, которое имеет только один делитель. Числами с ровно двумя делителями являются простые числа $n = p$: они делятся на 1 и на p . Наименьшим числом, имеющим два делителя, является, таким образом, $p = 2$.

Исследуем числа, имеющие ровно 3 делителя. В соответствии с (3.2.3) имеем

$$3 = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1).$$

Так как 3 — простое число, то справа может существовать лишь один множитель, не равный 1. Отсюда $r = 1$, а $\alpha_1 = 2$. Таким образом,

$$n = p_1^2.$$

Наименьшим числом с 3 делителями является $n = 2^2 = 4$. Это соображение, примененное к общему случаю, когда число делителей q является простым числом, позволяет получить, что

$$q = \alpha_1 + 1, \text{ т. е. } \alpha_1 = q - 1 \text{ и } n = p_1^{q-1};$$

наименьшим из таких чисел является

$$n = 2^{q-1}.$$

Рассмотрим следующий случай, когда существует ровно 4 делителя. Тогда соотношение

$$4 = (\alpha_1 + 1)(\alpha_2 + 1)$$

возможно только тогда, когда

$$\alpha_1 = 3, \alpha_2 = 0 \quad \text{или} \quad \alpha_1 = \alpha_2 = 1.$$

Это приводит к двум возможностям:

$$n = p_1^3, \quad n = p_1 \cdot p_2;$$

наименьшее число с 4 делителями — это $n = 6$.

В том случае, когда имеется 6 делителей, должно выполняться соотношение

$$6 = (\alpha_1 + 1)(\alpha_2 + 1),$$

что возможно лишь тогда, когда

$$\alpha_1 = 5, \quad \alpha_2 = 0 \quad \text{или} \quad \alpha_1 = 2, \quad \alpha_2 = 1.$$

Это дает две возможности:

$$n = p_1^5, \quad n = p_1^2 \cdot p_2;$$

при этом наименьшее значение имеет место в последнем случае, когда

$$p_1 = 2, \quad p_2 = 3, \quad n = 12.$$

Этот метод можно использовать для вычисления наименьших натуральных чисел, имеющих любое заданное количество делителей.

Существуют таблицы, указывающие количество делителей для различных чисел. Они начинаются следующим образом:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6

Вы легко можете ее самостоятельно продолжить.

Будем говорить, что натуральное число n является *сверхсоставным*, если количество делителей у каждого числа, меньшего n , меньше, чем количество делителей у числа n . Глядя на нашу небольшую таблицу, мы видим, что

$$1, 2, 4, 6, 12$$

являются первыми пятью сверхсоставными числами. О свойствах этих чисел известно еще очень мало.

Система задач 3.3.

1. Взвод из 12 солдат может маршировать 6-ю различными способами: 12×1 , 6×2 , 4×3 , 3×4 ,

2×6 , 1×12 . Какую наименьшую численность должны иметь группы людей, которые могут маршировать 8, 10, 12 и 72 способами?

2. Найдите наименьшие натуральные числа, имеющие: а) 14 делителей, б) 18 делителей и в) 100 делителей.

3. Найдите два первых сверхсоставных числа, следующих за числом 12.

4. Охарактеризуйте все натуральные числа, количество делителей которых является произведением двух простых чисел.

§ 4. Совершенные числа

Нумерология (или гематрия, как ее иногда еще называют) была распространенным увлечением у древних греков. Естественным объяснением этому является то, что числа в Древней Греции изображались буквами греческого алфавита, и поэтому каждому написанному слову, каждому имени соответствовало некоторое число. Люди могли сравнивать свойства чисел, соответствующих их именам.

Делители или *аликвотные части**) чисел играли важную роль в нумерологии. В этом смысле идеальными, или, как их называют, *совершенными* числами являлись такие числа, которые составлялись из своих аликвотных частей, т. е. равнялись сумме своих делителей. Здесь следует отметить, что древние греки не включали само число в состав его делителей.

Наименьшим совершенным числом является 6:

$$6 = 1 + 2 + 3.$$

За ним следует число 28:

$$28 = 1 + 2 + 4 + 7 + 14,$$

далее число 496:

$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248.$$

*) *Аликвотные дроби* — дроби вида $\frac{1}{n}$; в древности было принято всякую дробь представлять в виде суммы аликвотных дробей. Например, $\frac{5}{12} = \frac{1}{12} + \frac{1}{3}$. (Прим. перев.)

Часто математик, увлеченный решением какой-либо проблемы и имеющий одно или несколько частных решений этой задачи, пытается найти закономерности, которые смогли бы дать ключ к нахождению общего решения. Указанные нами совершенные числа могут быть записаны в виде

$$\begin{aligned}6 &= 2 \cdot 3 = 2(2^2 - 1), \\ 28 &= 2^2 \cdot 7 = 2^2(2^3 - 1), \\ 496 &= 2^4 \cdot 31 = 2^4(2^5 - 1).\end{aligned}$$

Это наталкивает нас на гипотезу:

Число является совершенным, если оно представляется в виде

$$P = 2^{p-1}(2^p - 1) = 2^{p-1}q, \quad (3.4.1)$$

где

$$q = 2^p - 1$$

является простым числом Мерсенна.

Этот результат, известный еще грекам, несложно доказать. Делителями числа P , включая само число P , очевидно, являются следующие числа:

$$\begin{aligned}1, \quad 2, \quad 2^2, \quad \dots, \quad 2^{p-1}, \\ q, \quad 2q, \quad 2^2q, \quad \dots, \quad 2^{p-1}q.\end{aligned}$$

Запишем сумму этих делителей

$$1 + 2 + \dots + 2^{p-1} + q(1 + 2 + \dots + 2^{p-1}),$$

которая равна

$$(1 + 2 + \dots + 2^{p-1})(q + 1) = (1 + 2 + \dots + 2^{p-1})2^p$$

Если вы не помните формулы для суммы членов геометрической прогрессии,

$$S = 1 + 2 + \dots + 2^{p-1},$$

то умножьте эту сумму на 2:

$$2S = 2 + 2^2 + \dots + 2^{p-1} + 2^p,$$

а затем, вычтя S , получите

$$S = 2^p - 1 = q.$$

Таким образом, сумма всех делителей числа P есть

$$2^p q = 2 \cdot 2^{p-1} q,$$

а сумма всех делителей, кроме самого числа $P = 2^{p-1}q$, равна

$$2 \cdot 2^{p-1}q - 2^{p-1}q = 2^{p-1}q = P.$$

Итак, наше число является совершенным.

Из этого результата следует, что каждое простое число Мерсенна порождает совершенное число. В § 2 второй главы говорилось, что известно всего 23 простых числа Мерсенна, следовательно, мы знаем также и 23 совершенных числа. Существуют ли другие виды совершенных чисел? Все совершенные числа вида (3.4.1) являются четными, можно доказать, что любое четное совершенное число имеет вид (3.4.1). Остается вопрос: существуют ли нечетные совершенные числа? В настоящее время мы не знаем ни одного такого числа, и вопрос о существовании нечетных совершенных чисел является одной из самых знаменитых проблем теории чисел. Если бы удалось обнаружить такое число, то это было бы крупным достижением. Вы можете поддаться соблазну найти такое число, перебирая различные нечетные числа. Но мы не советуем этого делать, так как по последним сообщениям Брайена Такхермана из IBM*) (1968), нечетное совершенное число должно иметь по крайней мере 36 знаков.

Система задач 3.4.

1. Используя список простых чисел Мерсенна, найдите четвертое и пятое совершенные числа.

§. 5. Дружественные числа

Дружественные числа также входят в наследство, доставшееся нам от греческой нумерологии. Если у двух людей имена были таковы, что их числовые значения удовлетворяли следующему условию: сумма частей (делителей) одного из них равнялась второму числу, и наоборот, то считалось, что это свидетельствует об их духовной близости. В действи-

*) Американская фирма, выпускающая вычислительное оборудование. (Прим. перев.)

тельности греки знали всего лишь одну пару таких чисел, а именно:

$$220 = 2^2 \cdot 5 \cdot 11, \quad 284 = 2^2 \cdot 71.$$

Суммами их делителей являются соответственно

$$1 + 2 + 4 + 5 + 10 + 20 + \\ + 11 + 22 + 44 + 55 + 110 = 284, \\ 1 + 2 + 4 + 71 + 142 = 220.$$

Эта пара дружественных чисел оставалась единственной известной до тех пор, пока Пьеру Ферма не удалось найти следующую пару:

$$17\,296 = 2^4 \cdot 23 \cdot 47, \quad 18\,416 = 2^4 \cdot 1151.$$

Поиски пар дружественных чисел чрезвычайно удобно вести с помощью ЭВМ. Для каждого числа n при помощи машины определяются все делители этого числа ($\neq n$) и их сумма m . После этого производится такая же операция с числом m . Если при этом вновь получается первоначальное число n , то пара чисел (n, m) оказывается дружественной. Недавно этим способом в Йельском университете на ЭВМ IBM 7094 были проверены все числа до одного миллиона. В результате была получена коллекция из 42 пар дружественных чисел; некоторые из них оказались ранее неизвестными. Все пары дружественных

Т а б л и ц а 2

Дружественные числа до 100 000

$220 = 2^2 \cdot 5 \cdot 11$	$284 = 2^2 \cdot 71$
$1184 = 2^5 \cdot 37$	$1210 = 2 \cdot 5 \cdot 11^2$
$2620 = 2^2 \cdot 5 \cdot 131$	$2924 = 2^2 \cdot 17 \cdot 43$
$5020 = 2^3 \cdot 2 \cdot 251$	$5564 = 2^2 \cdot 13 \cdot 107$
$6232 = 2^3 \cdot 19 \cdot 41$	$6368 = 2^5 \cdot 199$
$10744 = 2^3 \cdot 17 \cdot 79$	$10856 = 2^3 \cdot 23 \cdot 59$
$12285 = 3^3 \cdot 5 \cdot 7 \cdot 13$	$14595 = 3 \cdot 5 \cdot 7 \cdot 139$
$17296 = 2^4 \cdot 23 \cdot 47$	$18416 = 2^4 \cdot 1151$
$63020 = 2^2 \cdot 5 \cdot 23 \cdot 137$	$76084 = 2^2 \cdot 23 \cdot 827$
$66928 = 2^4 \cdot 47 \cdot 89$	$66992 = 2^4 \cdot 53 \cdot 79$
$67095 = 3^3 \cdot 5 \cdot 7 \cdot 71$	$71145 = 3^3 \cdot 5 \cdot 17 \cdot 31$
$69615 = 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17$	$87633 = 3^2 \cdot 7 \cdot 13 \cdot 107$
$79750 = 2 \cdot 5^3 \cdot 11 \cdot 29$	$88730 = 2 \cdot 5 \cdot 19 \cdot 467$

чисел до 100 000 приведены в табл. 2. При помощи этого метода, как нетрудно видеть, одновременно «вылавливаются» и совершенные числа. Если возникает желание продолжать поиски дальше, то, конечно, это можно сделать, но придется затратить большое количество машинного времени.

В действительности мы очень мало знаем о свойствах пар дружественных чисел, однако, можно на основе наших таблиц высказать несколько предположений. Например, отношение одного из них к другому, по-видимому, должно все больше и больше приближаться к 1 по мере того, как они увеличиваются. Из таблицы видно, что эти числа бывают либо оба четными, либо оба нечетными, но не было найдено случая, когда одно число четно, а другое нечетно, хотя поиски дружественных чисел такого вида были проведены среди всех чисел $n \leq 3\,000\,000\,000$.

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ И НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ

§ 1. Наибольший общий делитель

Откровенно говоря, мы надеемся, что многое в этой главе окажется для вас знакомым. В ней рассматриваются понятия, с которыми вы познакомились в школе, как только научились обращаться с обыкновенными дробями. Единственным оправданием включения этого материала является желание освежить его в вашей памяти. Мы также надеемся, что приведенное изложение материала явится более систематическим, чем то, к которому вы привыкли.

Возьмем некоторую дробь a/b , отношение двух целых положительных чисел a и b . Обычно мы стараемся привести ее к простейшему виду, т. е. мы стараемся сократить множители, общие для a и b . Эта операция не изменяет значения дроби, например,

$$\frac{24}{36} = \frac{8}{12} = \frac{2}{3}.$$

Общим делителем двух натуральных чисел a и b называется натуральное число d , которое является множителем как числа a , так и числа b , т. е.

$$a = d \cdot a_1, \quad b = d \cdot b_1.$$

Если число d — общий делитель чисел a и b , то он также делит числа $a + b$ и $a - b$, так как

$$\begin{aligned} a + b &= a_1 d + b_1 d = (a_1 + b_1) d, \\ a - b &= a_1 d - b_1 d = (a_1 - b_1) d. \end{aligned}$$

Когда известны разложения чисел a и b на простые множители, нетрудно найти все их общие делители. Выпишем эти два разложения на простые множители:

$$a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}, \quad b = p_1^{\beta_1} \cdot \dots \cdot p_r^{\beta_r}. \quad (4.1.1)$$

Здесь мы договариваемся записывать разложения чисел a и b так, как если бы они имели одинаковые простые множители

$$p_1, p_2, \dots, p_r,$$

но с условием, что мы допускаем возможность использования показателя степени, равного 0. Например, если p_1 делит число a , но не делит число b , мы полагаем, что в формуле (4.1.1) $\beta_1 = 0$. Таким образом, если

$$a = 140, \quad b = 110, \quad (4.1.2)$$

то

$$a = 2^2 \cdot 5^1 \cdot 7^1 \cdot 11^0, \quad b = 2^1 \cdot 5^1 \cdot 7^0 \cdot 11^1. \quad (4.1.3)$$

Из формулы (4.1.1) следует, что любой делитель d числа a может иметь простыми множителями только числа p_i , которые встречаются в числе a и каждое из них содержится в степени δ_i , не превосходящей соответствующей степени α_i в числе a . Аналогичные условия имеют место и для любого делителя d числа b . Поэтому общий делитель d чисел a и b может иметь в качестве простых множителей только числа p_i , которые встречаются одновременно в числах a и b , а степень δ_i числа p_i в d не может превышать меньшей из двух степеней: α_i и β_i .

Из этого обсуждения мы можем сделать вывод: любые два натуральных числа a и b имеют *наибольший общий делитель* d_0 . Простыми множителями p_i числа d_0 являются те, которые одновременно встречаются в числах a и b , а степень числа p_i в числе d_0 есть меньшее из двух чисел α_i и β_i .

Пример. Возьмем два числа, указанных в (4.1.2), имеющие разложения на простые множители (4.1.3); очевидно, что

$$d_0 = 2^1 \cdot 5^1 = 10.$$

Так как степень простого числа p_i в наибольшем общем делителе по крайней мере не меньше, чем у любого другого общего делителя, то мы получаем характеристическое свойство:

Любой общий делитель d делит наибольший общий делитель d_0 .

Наибольший общий делитель двух чисел настолько важен, что для него существует специальное обозначение:

$$d_0 = D(a, b). \quad (4.1.4)$$

Система задач 4.1.

1. Найдите наибольший общий делитель пар чисел: а) 360 и 1970, б) 30 и 365, в) номера вашего телефона и вашего почтового индекса.

2. Как бы вы стали доказывать, что $\sqrt{2}$ есть иррациональное число, используя в доказательстве теорему о единственности разложения?

§ 2. Взаимно простые числа

Число 1 является общим делителем для любой пары чисел a и b . Может случиться, что единица будет единственным их общим делителем, т. е.

$$d_0 = D(a, b) = 1. \quad (4.2.1)$$

В этом случае мы говорим, что числа a и b *взаимно простые*.

Пример. $(39, 22) = 1$.

Если числа имеют общий делитель, больший единицы, то они также имеют общий простой делитель. Итак, два числа могут быть взаимно простыми только тогда, когда они не имеют общих простых множителей, поэтому условие (4.2.1) означает, что числа a и b не имеют общих простых множителей, т. е. все их простые множители различны.

Вернемся к началу этой главы, где мы приводили дробь a/b к простейшему виду. Если d_0 есть наибольший общий делитель чисел a и b , то мы можем написать

$$a = a_0 d_0, \quad b = b_0 d_0. \quad (4.2.2)$$

Тогда

$$\frac{a}{b} = \frac{a_0 d_0}{b_0 d_0} = \frac{a_0}{b_0}. \quad (4.2.3)$$

В формуле (4.2.2) числа a_0 и b_0 не могут иметь простых общих множителей, в противном случае числа a и b имели бы общий множитель, больший, чем d_0 . Следовательно,

$$D(a_0, b_0) = 1. \quad (4.2.4)$$

Это означает, что для второй дроби в формуле (4.2.3) дальнейшее сокращение невозможно.

Одним из часто применяемых свойств взаимно простых чисел является следующее.

Если произведение ab делится на число c , которое взаимно просто с числом b , то число a делится на c .

Доказательство. Так как число c делит произведение ab , то простые множители числа c содержатся среди простых множителей чисел a и b . Но так как $D(b, c) = 1$, то их не может быть среди множителей числа b . Таким образом, все простые множители числа c делят число a , но не делят число b , и они появляются в числе a в степенях, не меньших, чем в числе c , так как число c делит ab .

Позже мы используем другой факт.

Если произведение двух взаимно простых чисел является квадратом,

$$ab = c^2, \quad D(a, b) = 1, \quad (4.2.5)$$

то числа a и b являются квадратами:

$$a = a_1^2, \quad b = b_1^2. \quad (4.2.6)$$

Доказательство. Для того чтобы некоторое число было квадратом, необходимо и достаточно, чтобы все степени в разложении его на простые множители были четными. Так как числа a и b — взаимно простые (4.2.5), то любой простой множитель из c^2 содержится либо в a , либо в b , но не в обоих; отсюда простые множители чисел a и b должны иметь четные степени.

Система задач 4.2.

1. Какие числа взаимно простые с числом 2?
2. Почему $D(n, n+1) = 1$?
3. Исследуйте пары дружественных чисел в табл. 2 (стр. 45) и найдите те из них, которые взаимно просты.
4. Может ли правило, выраженное в формулах (4.2.5) и (4.2.6), быть справедливым не только для квадратов, но и для произвольных степеней?

§ 3. Алгоритм Евклида

Вновь вернемся к нашим дробям a/b . Если $a > b$, то дробь является числом, большим 1, и мы часто разделяем ее на целую часть и правильную дробь, меньшую единицы.

Примеры. Мы пишем

$$\frac{32}{5} = 6 + \frac{2}{5} = 6 \frac{2}{5}, \quad \frac{63}{7} = 9 + \frac{0}{7} = 9.$$

В общем случае мы используем деление с остатком чисел a и b ($a \geq b$), а именно:

$$a = qb + r, \quad \text{где} \quad 0 \leq r \leq b - 1. \quad (4.3.1)$$

Очевидно, что это всегда возможно. Действительно, рассмотрим числа 0, 1, 2, ... на числовой прямой

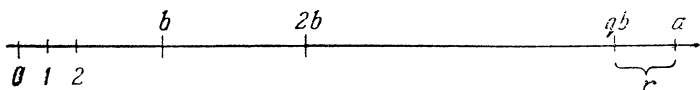


Рис. 14.

(рис. 14). Где-то на этой прямой расположено число a . Начиная от точки 0 станем отмечать точки b , $2b$, $3b$ и т. д. до точки qb такой, что qb не больше, чем a , в то время как $(q+1)b$ уже больше a . Расстояние от точки qb до точки a и есть r . Мы называем число r *остатком* при делении (4.3.1), а q — *частным*. Это частное q встречается столь часто, что имеется специальный символ для его обозначения:

$$q = \left[\frac{a}{b} \right].$$

Этот символ обозначает *наибольшее целое число, не превосходящее числа a/b* . Для примеров, приведенных выше, получим

$$\left[\frac{32}{5} \right] = 6, \quad \left[\frac{63}{7} \right] = 9.$$

В предыдущем разделе мы исследовали наибольший общий делитель двух натуральных чисел a и b :

$$d_0 = D(a, b). \quad (4.3.2)$$

Чтобы найти число d_0 , мы полагали, что мы знаем разложения чисел a и b на простые множители. Однако нахождение таких разложений может оказаться очень трудным занятием для больших чисел. Существует совсем другой метод для нахождения наибольшего общего делителя, который не использует подобных разложений. Он основан на следующем:

Если $a = qb + r$, где $0 \leq r \leq b - 1$, то

$$D(a, b) = d = D(r, b). \quad (4.3.3)$$

Доказательство. Запишем

$$d_0 = D(a, b), \quad d_1 = D(r, b).$$

Таким образом, доказательство соотношения (4.3.3) означает доказательство того, что $d_0 = d_1$. Любой общий делитель чисел a и b также делит число

$$r = a - qb.$$

Следовательно, число r делится на d_0 .

Так как число d_0 является делителем как числа r , так и числа b , то оно должно делить и число $d_1 = D(b, r)$; отсюда $d_1 \geq d_0$. С другой стороны, в соответствии с соотношением (4.3.1) любой общий делитель чисел r и b делит число a , откуда число d_1 делит число a . Так как число d_1 делит также и число b , то оно должно делить и число $d_0 = D(a, b)$, следовательно, $d_0 \geq d_1$. Из сказанного следует, что $d_0 = d_1$.

Пример. $1066 = 5 \cdot 200 + 66$; следовательно, $(1066, 200) = (66, 200)$.

Этот результат, сформулированный в утверждении (4.3.3), дает нам простой метод вычисления наибольшего общего делителя двух чисел. Вместо поисков наибольшего общего делителя чисел a и b достаточно найти наибольший общий делитель чисел r и b . Эта задача более проста, так как число r меньше, чем каждое из чисел a и b . Чтобы найти наибольший общий делитель чисел r и b , мы вновь воспользуемся тем же методом и разделим число b на r :

$$b = q_1 r + r_1,$$

где r_1 меньше каждого из чисел b и r . В соответствии с правилом (4.3.3) мы получаем

$$d_0 = D(a, b) = D(b, r) = D(r, r_1).$$

Далее, таким же способом обращаемся с числами r и r_1 и т. д. В результате получаем последовательность пар чисел, каждая из которых имеет один и тот же наибольший общий делитель:

$$\begin{aligned} d_0 = D(a, b) &= D(b, r) = \\ &= D(r, r_1) = D(r_1, r_2) = \dots \end{aligned} \quad (4.3.4)$$

Так как остатки постоянно уменьшаются, то эта последовательность должна закончиться после получения остатка $r_{k+1} = 0$. Это происходит при делении

$$r_{k-1} = q_{k+1}r_k + 0,$$

т. е. число r_k делит число r_{k-1} . Тогда

$$D(r_{k-1}, r_k) = r_k,$$

и из (4.3.4) видим, что

$$d_0 = D(a, b) = r_k.$$

Другими словами, число d_0 равно первому из остатков, который делит предшествующий ему остаток.

Пример. Найдем наибольший общий делитель чисел 1970 и 1066. Когда мы разделим одно число на другое и продолжим этот процесс дальше, как было выше рассказано, то найдем

$$1970 = 1 \cdot 1066 + 904,$$

$$1066 = 1 \cdot 904 + 162,$$

$$904 = 5 \cdot 162 + 94,$$

$$162 = 1 \cdot 94 + 68,$$

$$94 = 1 \cdot 68 + 26,$$

$$68 = 2 \cdot 26 + 16,$$

$$26 = 1 \cdot 16 + 10,$$

$$16 = 1 \cdot 10 + 6,$$

$$10 = 1 \cdot 6 + 4,$$

$$6 = 1 \cdot 4 + 2,$$

$$4 = 2 \cdot 2 + 0.$$

Следовательно, $(1970, 1066) = 2$.

Этот метод нахождения наибольшего общего делителя двух чисел называется *алгоритмом Евклида*, так

как первое его описание содержится в «Началах» Евклида. Этот метод очень удобен для применения в вычислительных машинах.

Система задач 4.3.

1. Решите задачу 1 § 1 (с. 49), используя алгоритм Евклида.

2. Найдите наибольший общий делитель для каждой из пяти первых пар дружественных чисел. Сравните результаты с результатами, полученными с помощью разложения на простые множители.

3. Каким количеством нулей заканчивается число

$$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n?$$

Сверьте свой результат с таблицей факториалов.

§ 4. Наименьшее общее кратное

Вновь вернемся к дробям. Чтобы сложить (или вычесть) две дроби

$$\frac{c}{a}, \frac{d}{b},$$

мы приводим их к общему знаменателю, а затем складываем (или вычитаем) числители.

Пример.

$$\frac{2}{15} + \frac{5}{9} = \frac{6}{45} + \frac{25}{45} = \frac{31}{45}.$$

Вообще, чтобы получить сумму

$$\frac{c}{a} + \frac{d}{b},$$

мы должны найти общее кратное для чисел a и b , т. е. число m , на которое делятся как число a , так и b . Одно из таких чисел очевидно, а именно, их произведение $m = ab$; в результате получаем в качестве суммы дробей

$$\frac{c}{a} + \frac{d}{b} = \frac{cb}{ab} + \frac{da}{ab} = \frac{cb + da}{ab}.$$

Но существует бесконечно много других общих кратных для чисел a и b . Предположим, что мы знаем разложение этих двух чисел на простые множители:

$$a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}, \quad b = p_1^{\beta_1} \cdot \dots \cdot p_r^{\beta_r}. \quad (4.4.1)$$

Число m , которое делится одновременно на числа a и b , должно делиться на каждый простой делитель p_i чисел a и b и содержать его в степени μ_i не меньшей, чем большая из двух степеней α_i и β_i . Таким образом, среди общих кратных существует наименьшее

$$m_0 = p_1^{\mu_1} \cdot \dots \cdot p_r^{\mu_r}, \quad (4.4.2)$$

в котором каждый показатель степени μ_i равен большему из чисел α_i и β_i . Очевидно, что число m_0 является *наименьшим общим кратным* и любое другое общее кратное чисел a и b делится на m_0 . Для наименьшего общего кратного существует специальное обозначение

$$m_0 = K(a, b). \quad (4.4.3)$$

Пример. $a = 140$, $b = 110$. Разложение на простые множители этих чисел таково:

$$a = 2^2 \cdot 5^1 \cdot 7^1 \cdot 11^0, \quad b = 2^1 \cdot 5^1 \cdot 7^0 \cdot 11^1,$$

следовательно,

$$K(a, b) = 2^2 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 1540.$$

Существует следующее простое соотношение между наибольшим общим делителем и наименьшим общим кратным:

$$ab = D(a, b) K(a, b). \quad (4.4.4)$$

Доказательство. Перемножив два числа из (4.4.1), получим

$$ab = p_1^{\alpha_1 + \beta_1} \cdot \dots \cdot p_r^{\alpha_r + \beta_r}. \quad (4.4.5)$$

Как мы отмечали, степень числа p_i в $D(a, b)$ является меньшей из двух чисел α_i и β_i , а в числе $K(a, b)$ она большая из них. Предположим, что $\alpha_i \leq \beta_i$. Тогда степень числа p_i в числе $D(a, b)$ равна α_i , а в $K(a, b)$ равна β_i ; следовательно, в их произведении

$$D(a, b) \cdot K(a, b)$$

она равна $\alpha_i + \beta_i$, что в точности равняется степени в произведении (4.4.5). Это показывает справедливость соотношения (4.4.4).

Пример. $a = 140$, $b = 110$, $D(a, b) = 10$, $K(a, b) = 1540$.

$$ab = 140 \cdot 110 = 10 \cdot 1540 = D(a, b) K(a, b).$$

Из правила (4.4.4) вытекает, что если a и b взаимно простые, то их произведение равно их наибольшему общему кратному; действительно, в этом случае $D(a, b) = 1$ и поэтому $ab = K(a, b)$.

Система задач 4.4.

1. Найдите наибольшее общее кратное пар чисел в системе задач 4.1 (с. 49).

2. Найдите наибольшее общее кратное для каждой из четырех первых пар дружественных чисел.

ЗАДАЧА ПИФАГОРА

§ 1. Предварительные замечания

Во введении (§ 3, гл. 1) мы упоминали об одной из древнейших теоретико-числовых задач: найти все прямоугольные треугольники с целочисленными сторонами, т. е. найти все целочисленные решения уравнения

$$x^2 + y^2 = z^2. \quad (5.1.1)$$

Эта задача может быть решена с использованием лишь простейших свойств чисел. Прежде чем приступить к ее решению, проведем некоторые предварительные исследования. Тройка целых чисел

$$(x, y, z), \quad (5.1.2)$$

удовлетворяющая уравнению (5.1.1), называется *пифагоровой тройкой*. Отбросим тривиальный случай, когда одна из сторон треугольника равна нулю.

Ясно, что если множество (5.1.2) является пифагоровой тройкой, то любая тройка чисел

$$(kx, ky, kz), \quad (5.1.3)$$

получающаяся умножением каждого из этих чисел на некоторое целое число k , также будет пифагоровой, и наоборот. Таким образом, при поиске решений достаточно ограничиться нахождением *простейших треугольников*, длины сторон которых не имеют общего множителя $k > 1$. Например, тройки

$$(6, 8, 10), \quad (15, 20, 25)$$

являются пифагоровыми тройками, получающимися из простейшего решения (3, 4, 5).

В простейшей тройке (x, y, z) не существует общего множителя для всех трех чисел. В действитель-

ности справедливо более сильное утверждение: никакие два числа из простейшей тройки не имеют общего множителя, т. е.

$$D(x, y) = 1, \quad D(x, z) = 1, \quad D(y, z) = 1. \quad (5.1.4)$$

Чтобы доказать это, предположим, что, например, x и y имеют общий делитель. Тогда они имеют общий простой делитель p . В соответствии с (5.1.1) число p должно также делить и z . Итак, (x, y, z) не может быть простейшей тройкой. Такие же рассуждения применимы для доказательства остальных двух утверждений.

Рассмотрим еще ряд свойств простейших троек. Мы только что получили, что числа x и y не могут быть оба четными, но мы можем также показать, что они не могут быть и оба нечетными. Действительно, предположим, что

$$x = 2a + 1, \quad y = 2b + 1.$$

После возведения в квадрат этих чисел и сложения их, получим число

$$\begin{aligned} x^2 + y^2 &= (2a + 1)^2 + (2b + 1)^2 = \\ &= 2 + 4a + 4a^2 + 4b + 4b^2 = 2 + 4(a + a^2 + b + b^2), \end{aligned}$$

делящееся на 2, но не делящееся на 4. В соответствии с (5.1.1) это означает, что z^2 делится на 2, но не делится на 4, но это невозможно, так как если z^2 делится на 2, то и z делится на 2, но тогда z^2 делится на 4.

Так как одно из чисел x и y — четное, а другое — нечетное, то z — также нечетное. *Для определенности будем считать, что в наших обозначениях число x — четное, а y — нечетное.*

§ 2. Решение задачи Пифагора

Чтобы найти простейшие решения уравнения Пифагора (5.1.1), перепишем его в виде

$$x^2 = z^2 - y^2 = (z + y)(z - y). \quad (5.2.1)$$

Вспоминая, что x — четное, а y и z — оба нечетные, получаем, что все три числа

$$x, \quad z + y, \quad z - y$$

четные. Тогда мы можем разделить обе части уравнения (5.2.1) на 4 и получить

$$\left(\frac{1}{2}x\right)^2 = \frac{1}{2}(z+y) \cdot \frac{1}{2}(z-y). \quad (5.2.2)$$

Обозначим

$$m_1 = \frac{1}{2}(z+y), \quad n_1 = \frac{1}{2}(z-y); \quad (5.2.3)$$

тогда уравнение (5.2.2) переписывается как

$$\left(\frac{1}{2}x\right)^2 = m_1 n_1. \quad (5.2.4)$$

Числа m_1 и n_1 взаимно простые. Чтобы это увидеть, предположим, что

$$d = D(m_1, n_1)$$

есть наибольший общий делитель чисел m_1 и n_1 . Тогда, как это следует из § 1 гл. 4, число d должно делить оба числа

$$m_1 + n_1 = z, \quad m_1 - n_1 = y.$$

Но единственным общим делителем чисел z и y в простейшей тройке может быть только 1, поэтому

$$d = D(m_1, n_1) = 1. \quad (5.2.5)$$

Так как произведение (5.2.4) этих двух взаимно простых чисел является квадратом, то можно использовать результат, изложенный в конце § 2 гл. 4 (стр. 50), согласно которому числа m_1 и n_1 являются квадратами

$$m_1 = m^2, \quad n_1 = n^2, \quad D(m, n) = 1. \quad (5.2.6)$$

Здесь мы можем без нарушения общности считать, что $m > 0$, $n > 0$. Теперь подставим m^2 и n^2 вместо m_1 и n_1 соответственно в уравнения (5.2.3) и (5.2.4); получим

$$m^2 = \frac{1}{2}z + \frac{1}{2}y, \quad n^2 = \frac{1}{2}z - \frac{1}{2}y, \quad m^2 n^2 = \frac{1}{4}x^2,$$

т. е.

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2. \quad (5.2.7)$$

Проверка показывает, что эти три числа всегда удовлетворяют соотношению Пифагора $x^2 + y^2 = z^2$.

Осталось определить, какие целые положительные числа m и n в действительности соответствуют простейшим треугольникам. Докажем, что следующие три условия на числа m и n являются необходимыми и достаточными:

- (1) $(m, n) = 1,$
- (2) $m > n,$ (5.2.8)
- (3) одно из чисел m и n четное, а другое — нечетное.

Доказательство. Сначала покажем, что если числа x, y, z образуют простейшую тройку, то условия (5.2.8) выполняются. Мы уже показали, что условие (1) является следствием того, что числа x, y, z взаимно простые. Условие (2) следует из того, что числа x, y, z — положительные. Чтобы увидеть, что условие (3) необходимо, заметим, что если m и n оба нечетные, то в соответствии с (5.2.7) y и z были бы оба четные, в противоречие с результатами, полученными в конце предыдущего параграфа.

Наоборот, если условия (5.2.8) выполнены, то соотношения (5.2.7) определяют простейшую тройку; условие (2) обеспечивает положительность чисел x, y и z .

Могут ли какие-нибудь два из этих трех чисел иметь общий простой множитель p ? Такое простое число p , делящее два из них, должно также делить и третье в силу соотношения $x^2 + y^2 = z^2$. Если число p делит x , то оно в соответствии с (5.2.7) должно делить $2mn$. Число p не может равняться 2, потому что y и z нечетные в соответствии с условием (3) и (5.2.7). Предположим, что $p \neq 2$ — нечетное простое число, делящее m . Тогда условие (1) и выражение (5.2.7) показывают, что p не может делить y и z . Такие же рассуждения применимы и для случая, если p делит число n .

Найдем необходимые и достаточные условия (5.2.8) для того, чтобы m и n давали простейший треугольник, можно вычислить все такие треугольники с помощью соотношения (5.2.7). Например, пусть

$$m = 11, \quad n = 8.$$

Наши условия выполнены, и мы находим, что

$$x = 176, \quad y = 57, \quad z = 185.$$

В табл. 3 приведены все простейшие треугольники x, y, z для нескольких первых значений чисел m и n .

Таблица 3

$\begin{matrix} m \\ n \end{matrix}$	2	3	4	5	6	7
1	4,3,5		8,15,17		12,35,37	
2		12,5,13	24,7,25	20,21,29		28,45,53
3				40,9,41		56,33,65
4					60,11,61	
5						84,13,85
6						

Система задач 5.2.

1. Продлите таблицу для всех значений $m \leq 10$.
2. Могут ли два разных набора значений чисел m и n , удовлетворяющих условию (5.2.8), дать один и тот же треугольник?
3. Найдите все пифагоровы треугольники, у которых длина гипотенузы не превосходит 100.

§ 3. Несколько задач о треугольниках Пифагора

Мы решили задачу нахождения всех треугольников Пифагора. Здесь, как почти всегда в математике, решение одной задачи приводит к постановке ряда других задач. Часто новые вопросы оказываются значительно более трудными, чем первоначальный.

Одним из естественных вопросов о простейших треугольниках является следующий. Пусть задана одна из сторон простейшего треугольника Пифагора, как найти остальные? Первым рассмотрим случай, когда известна сторона y . В соответствии с (5.2.7)

$$y = m^2 - n^2 = (m + n)(m - n), \quad (5.3.1)$$

где m и n — числа, удовлетворяющие условиям (5.2.8). В уравнении (5.3.1) множители $(m + n)$ и $(m - n)$ взаимно простые. Чтобы в этом убедиться, заметим, что эти множители

$$a = m + n, \quad b = m - n \quad (5.3.2)$$

оба нечетные, так как одно из чисел m и n нечетное, а другое четное. Если числа a и b имеют общий нечетный простой множитель p , то число p должно было бы делить каждое из чисел

$$a + b = m + n + (m - n) = 2m$$

и

$$a - b = m + n - (m - n) = 2n,$$

т. е. p должно было бы делить числа m и n . Но это невозможно, так как $D(m, n) = 1$.

Предположим теперь, что есть разложение данного нечетного числа y на два множителя

$$y = a \cdot b, \quad a > b, \quad D(a, b) = 1. \quad (5.3.3)$$

Из (5.3.2) получаем

$$m = \frac{1}{2}(a + b), \quad n = \frac{1}{2}(a - b). \quad (5.3.4)$$

Эти два числа также взаимно простые, поскольку любой их общий множитель должен был бы делить числа $a = m + n$ и $b = m - n$. Кроме того, числа m и n не могут быть оба нечетными, ибо тогда каждое из чисел a и b делилось бы на 2. Отсюда заключаем, что числа m и n удовлетворяют условиям (5.2.8) и, таким образом, определяют простейший треугольник, одна из сторон которого $y = m^2 - n^2$.

Пример. Пусть $y = 15$. Для него существуют два разложения на множители, удовлетворяющие условиям (5.3.3), а именно:

$$y = 15 \cdot 1 = 5 \cdot 3.$$

Первое из них дает

$$m = 8, \quad n = 7, \quad x = 112, \quad y = 15, \quad z = 113,$$

а второе

$$m = 4, \quad n = 1, \quad x = 8, \quad y = 15, \quad z = 17.$$

Пусть, далее, задана сторона x . Так как какое-то из чисел m или n делится на 2, то очевидно, что $x = 2mn$ должно делиться на 4. Если разложить число $x/2$ на два взаимно простых множителя, то больший из них можно взять в качестве числа m , а меньший — n .

Пример. Возьмем $x = 24$; тогда

$$\frac{1}{2}x = 12 \cdot 1 = 4 \cdot 3.$$

Первое разложение дает

$$m = 12, \quad n = 1, \quad x = 24, \quad y = 143, \quad z = 145,$$

а второе

$$m = 4, \quad n = 3, \quad x = 24, \quad y = 7, \quad z = 25.$$

Третий и последний случай приводит нас к необходимости коснуться одной важной задачи теории чисел. Если z — гипотенуза простейшего треугольника Пифагора, то в соответствии с (5.2.7) имеем

$$z = m^2 + n^2, \quad (5.3.5)$$

т. е. число z есть сумма квадратов чисел m и n , удовлетворяющих условиям (5.2.8).

Это приводит нас к постановке вопроса, уже решенного П. Ферма: *когда целое число можно представить в виде суммы квадратов двух целых чисел*:

$$z = a^2 + b^2? \quad (5.3.6)$$

На время забудем все ограничения на числа a и b . Пусть они могут иметь общие множители, а также каждое из них, или даже сразу оба могут обращаться в нуль. Перечислим все целые числа, меньшие десяти, представляемые в виде суммы двух квадратов:

$$\begin{aligned} 0 &= 0^2 + 0^2, & 1 &= 1^2 + 0^2, & 2 &= 1^2 + 1^2, \\ 4 &= 2^2 + 0^2, & 5 &= 2^2 + 1^2, & 8 &= 2^2 + 2^2, \\ 9 &= 3^2 + 0^2, & 10 &= 3^2 + 1^2. \end{aligned}$$

Оставшиеся числа 3, 6 и 7 не представляются в виде суммы двух квадратов.

Опишем, как можно выяснить, является ли число суммой двух квадратов. К сожалению, мы не можем привести здесь доказательства ввиду его сложности.

Рассмотрим вначале простые числа. Каждое простое число вида $p = 4n + 1$ всегда является суммой двух квадратов; например,

$$\begin{aligned} 5 &= 2^2 + 1^2, & 13 &= 3^2 + 2^2, & 17 &= 4^2 + 1^2, \\ 29 &= 5^2 + 2^2. \end{aligned}$$

Существенно, что такое представление может осуществляться единственным способом.

Остальные нечетные простые числа имеют вид $q = 4n + 3$, т. е.

$$q = 3, 7, 11, 19, 23, 31, \dots$$

Ни одно такое простое число не представляется в виде суммы двух квадратов; более того, вообще ни одно число вида $4n + 3$ не может быть представлено в виде суммы двух квадратов. Чтобы убедиться в этом, заметим, что если целые числа a и b оба четные, то a^2 и b^2 оба делятся на 4, отсюда и $a^2 + b^2$ делится на 4. Если они оба нечетные, например, $a = 2k + 1$, $b = 2l + 1$, то $a^2 + b^2 = 4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 4(k^2 + l^2 + k + l) + 2$, поэтому $a^2 + b^2$ имеет при делении на 4 остаток 2. И наконец, если одно из целых чисел a и b четное, а другое — нечетное, скажем, $a = 2k + 1$, $b = 2l$, то

$$a^2 + b^2 = 4k^2 + 4k + 1 + 4l^2$$

и имеет при делении на 4 остаток 1. Итак, мы перебрали все возможности и можем заключить, что сумма двух квадратов никогда не представима в виде $4n + 3$.

Чтобы закончить наше исследование для простых чисел, заметим, что $2 = 1^2 + 1^2$.

Для того чтобы проверить, является ли составное число z суммой двух квадратов, разложим его на простые множители

$$z = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}. \quad (5.3.7)$$

Число z оказывается суммой двух квадратов тогда и только тогда, когда каждое простое число p_i вида $4n + 3$ входит в разложение в четной степени.

Примеры. Число $z = 198 = 2 \cdot 3^2 \cdot 11$ не является суммой двух квадратов, так как 11 имеет вид $4n + 3$ и входит в разложение в первой степени.

Число $z = 194 = 2 \cdot 97$ является суммой двух квадратов, так как ни один из его простых множителей не является числом вида $4n + 3$. Действительно,

$$z = 13^2 + 5^2.$$

Вернемся к нашей первоначальной задаче нахождения всех чисел z , которые могут быть гипотену-

зами простейших треугольников Пифагора. Такое число z должно быть представимо в виде $z = m^2 + n^2$, где числа m и n удовлетворяют условиям (5.2.8). Необходимым и достаточным условием для этого является следующее: каждый из простых множителей числа z должен иметь вид $4n + 1$. Доказательство этого утверждения мы вновь опускаем.

Примеры. $z = 41$. Это число легко представить в виде суммы двух квадратов искомого вида, $z = 5^2 + 4^2$, так что $m = 5$, $n = 4$ и $x = 40$, $y = 9$, $z = 41$ выражают длины сторон соответствующего треугольника.

$z = 1105 = 5 \cdot 13 \cdot 17$. Существуют четыре представления этого числа в виде суммы двух квадратов:

$1105 = 33^2 + 4^2 = 32^2 + 9^2 = 31^2 + 12^2 = 24^2 + 23^2$.
Стороны соответствующих треугольников вычислите самостоятельно.

Целый ряд задач о треугольниках Пифагора может быть решен при помощи наших формул (5.2.7)

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2.$$

Например, можно искать треугольники Пифагора с заданной площадью A . Если такой треугольник является простейшим, то его площадь равна

$$A = \frac{1}{2} xy = mn(m - n)(m + n). \quad (5.3.8)$$

Здесь три из четырех множителей нечетны. Нетрудно видеть, что они попарно взаимно простые. Поэтому, чтобы найти все возможные значения чисел m и n , можно выделить из числа A два взаимно простых нечетных множителя k и l ($k > l$), положив

$$m + n = k, \quad m - n = l,$$

что дает

$$m = \frac{1}{2}(k + l), \quad n = \frac{1}{2}(k - l).$$

После этого мы проверяем, удовлетворяют ли эти числа условиям (5.3.8).

Рассуждения несколько упрощаются, если заметить, что два множителя в выражении (5.3.8) могут равняться 1 только в единственном случае:

$$m = 2, \quad n = 1, \quad A = 6.$$

Действительно, два множителя в (5.3.8) могут быть равны 1, только если

$$n = m - n = 1,$$

что и дает указанное выше значение.

Пример. Найдем все треугольники Пифагора с площадью $A = 360$. Разложение числа A на простые множители таково: $A = 2^3 \cdot 3^2 \cdot 5$. Число A может быть единственным образом записано в виде произведения четырех взаимно простых множителей: $A = 8 \cdot 1 \cdot 5 \cdot 9$. Если мы ищем простейший треугольник, то $m + n = 9$. Однако если $m = 8$, то $n = 1$ и $m - n = 7$, но A не делится на 7, а вторая возможность ($n = 8$, $m = 1$) исключается условием $m > n$. Поэтому такого треугольника не существует.

Этот результат не исключает возможности существования треугольников с площадью $A = 360$, не являющихся простейшими. Следующее соображение может быть использовано в общем случае для нахождения треугольников заданной площади, не являющихся простейшими. Если длины всех сторон треугольника имеют общий делитель d , т. е. могут быть записаны как

$$dx, \quad dy, \quad dz,$$

то его площадь равна

$$A = \frac{1}{2} dx dy = d^2 mn (m - n) (m + n).$$

Таким образом, число d^2 является множителем числа A и, если число d есть наибольший общий делитель длин сторон, то число

$$A_0 = \frac{A}{d^2} = mn (m - n) (m + n)$$

должно быть площадью простейшего треугольника.

Применим полученный результат к только что рассмотренному случаю $A = 360$. У этого числа существуют три множителя, являющиеся квадратами:

$$d_1 = 4, \quad d_2 = 9, \quad d_3 = 36.$$

Соответственно находим

$$\frac{A}{d_1} = 90 = 2 \cdot 3^2 \cdot 5, \quad \frac{A}{d_2} = 40 = 2^3 \cdot 5, \quad \frac{A}{d_3} = 10 = 2 \cdot 5.$$

Не существует способов написать число 40 или 10 в виде произведения четырех взаимно простых множителей, а число 90 может быть представлено в таком виде, причем единственным образом, а именно:

$$90 = 1 \cdot 2 \cdot 3^2 \cdot 5.$$

(В числе сомножителей 1 может встречаться не более одного раза, за исключением случая $m = 2$, $n = 1$, $A = 6$.) Так как наибольшим множителем является 9, то мы должны взять $m + n = 9$. Однако, перебирая все возможные значения $m = 1, 2, 5$, получим соответственно $n = 8, 7, 4$. Условие $m > n$ исключает все случаи, кроме $m = 5$, $n = 4$, для которого, однако, $mn(m + n)(m - n) \neq 90$. Итак, мы получили, что не существует ни простейшего, ни иного треугольника Пифагора с площадью $A = 360$.

Можно было бы затронуть еще много других вопросов, но упомянем лишь об одном из них. Периметр треугольника равен

$$c = x + y + z; \quad (5.3.9)$$

для простейшего треугольника Пифагора получаем

$$c = 2mn + (m^2 - n^2) + (m^2 + n^2) = 2m(m + n).$$

Мы предоставляем читателю самому отыскать метод нахождения всех треугольников Пифагора с заданным периметром. Не пренебрегайте рассмотрением числовых примеров.

Мы решили задачу построения всех треугольников Пифагора. Это ведет нас к исследованию более общих связанных с ней задач. Естественным обобщением задачи Пифагора является *задача Герона*, названная по имени древнегреческого математика Герона, жившего в Александрии: *найти все треугольники с целочисленными сторонами, площади которых также выражаются целыми числами*. Эта задача отличается от задачи Пифагора тем, что условие наличия прямого угла заменено требованием целочисленности площади. Очевидно, что всякий треугольник Пифагора удовлетворяет условиям задачи Герона.

Для проверки того, является ли данный треугольник треугольником Герона, проще всего применить

формулу Герона для площади треугольника,

$$A = \sqrt{\frac{1}{2}c\left(\frac{1}{2}c - x\right)\left(\frac{1}{2}c - y\right)\left(\frac{1}{2}c - z\right)},$$

где c — это периметр треугольника, определенный в (5.3.9). Хотя известно значительное число треугольников Герона, не существует общей формулы, описывающей все эти треугольники. Приведем несколько из них (не прямоугольных):

$x = 7$	$y = 15$	$z = 20$
9	10	17
13	14	15
39	41	50

Мы не можем закончить рассказ о треугольниках Пифагора, не упомянув об одной из самых знаменитых проблем математики, гипотезе П. Ферма:

для $n > 2$ не существует натуральных чисел x , y , z таких, что

$$x^n + y^n = z^n.$$

Эта идея пришла к Ферма в то время, когда он изучал перевод с греческого «Арифметики» Диофанта. В этой книге в основном рассматриваются задачи, в решении которых применяются формулы для нахождения треугольников Пифагора. Читая эту книгу, Ферма делал пометки на полях.

Ферма был взволнован своим «открытием», он верил, что у него есть удивительное доказательство, и сожалел, что не может его записать, так как поля слишком узки. С тех пор эта задача занимает математиков. Для нахождения доказательства изобретались самые искусные методы; этот поиск привел к открытию новых фундаментальных теорий в математике. Используя теоретические разработки и вычисления на ЭВМ, было показано, что теорема Ферма справедлива для многих значений степени n . В настоящее время мы знаем, что этот результат выполняется для всех значений n , удовлетворяющих неравенству $3 \leq n \leq 4002$.

Попытки самых выдающихся математиков в течение столетий найти общее доказательство оказались тщетными. Поэтому распространилось мнение, что

Ферма, несмотря на свой бесспорный талант, стал жертвой самообмана. Как бы ни широки были поля книги, маловероятно, что его доказательство было бы верным.

Конечно, вы имеете право попробовать свои силы в доказательстве этой теоремы, но предупреждаем, что еще ни одна теорема в математике не имела столько неправильных доказательств, как теорема Ферма. Лишь некоторые из них принадлежат хорошим математикам, остальные — дилетантам. Доказательства «последней теоремы Ферма» продолжают появляться в почте известных математиков, занимающихся теорией чисел. Большинство из этих доказательств сопровождается письмами с требованием о немедленном всемирном признании и выплате денежной премии, установленной одним немецким математиком (эта премия давно уже обесценилась в результате инфляций).

Система задач 5.3.

1. Найдите все такие треугольники Пифагора, у которых длина одной из сторон равна: а) 50, б) 22.

2. Используя условие представимости числа в виде суммы двух квадратов, определите, какие из чисел 100, 101, ..., 110 могут быть представлены в таком виде. Если возможно, найдите все представления. Какое из этих чисел может быть гипотенузой простейшего треугольника Пифагора?

3. Могут ли быть треугольниками Пифагора треугольники с площадями $A = 78$, $A = 120$, $A = 1000$?

4. Найдите все треугольники Пифагора с периметрами $c = 88$, $c = 110$.

СИСТЕМЫ СЧИСЛЕНИЯ

§ 1. Числа

«Все есть число» — учили древние пифагорейцы *). Однако количество чисел, которыми они пользовались, ничтожно по сравнению с фантастической пляской цифр, окружающих нас сегодня в повседневной жизни. Огромные числа появляются, когда считаем мы, и тогда, когда считают нас. В нашу жизнь прочно вошли: номера домов, квартир, телефонов, счетов, почтовые индексы. Каждый день наполнен потоком счетов, чеков и других бухгалтерских документов. Государственный бюджет исчисляется в миллиардах, а горы статистических данных являются принятым доводом в спорах. Эти цифры «крутятся» в компьютерах, которые анализируют состояние производства, следят за траекториями спутников и исследуют атомные ядра со скоростью до одного миллиарда операций в секунду.

Ко всему этому вела длинная дорога, начавшаяся с первых попыток человека систематизировать окружающие его числа, когда они стали столь большими, что их нельзя уже было посчитать на пальцах. Были перепробованы различные способы группировки чисел; большинство из них осталось на обочине этого пути, не выдержав конкуренции с другими системами. К настоящему времени, по счастью, наша десятичная, или десятичная, система счисления, основанная на группировании десятками, принята почти всюду; в некотором отношении эта система, по-видимому, случайно, оказалась той золотой серединой, которая одинаково хорошо удовлетворяет разнообразным требованиям при работе с числами.

*) Последователи философской школы Пифагора. (Прим. перев.)

Нет необходимости подробно описывать эту систему. Первые два года обучения в школе дают нам на всю жизнь почти подсознательное знание того, что означает последовательность цифр, например,

$$\begin{aligned}75 &= 7 \cdot 10 + 5, \\1066 &= 1 \cdot 10^3 + 0 \cdot 10^2 + 6 \cdot 10 + 6, \\1970 &= 1 \cdot 10^3 + 9 \cdot 10^2 + 7 \cdot 10 + 0.\end{aligned}$$

И вообще, в системе, основанной на числе 10,

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} \quad (6.1.1)$$

означает число

$$\begin{aligned}N &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots \\&\dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0, \quad (6.1.2)\end{aligned}$$

где коэффициенты, или цифры, a_i могут принимать следующие значения:

$$a_i = \{0, 1, \dots, 9\}. \quad (6.1.3)$$

Число $b = 10$ называется *основанием этой системы*. Индо-арабская числовая система пришла в Европу с Востока около 1200 г. нашей эры, и с тех пор не оспаривалась. Она известна как *позиционная система*, так как место каждой цифры определяет ее значение; использование символа 0 дает возможность просто и безболезненно обозначать пустующее место. Более того, оказалось, что эта система очень удобна при арифметических операциях с числами: сложении, вычитании, умножении и делении.

§ 2. Другие системы

Известны различные другие системы, которыми пользовались народы мира, чтобы навести порядок среди чисел. Но почему и как возникли эти системы? Ответы на эти вопросы большей частью затерялись в туманном прошлом человечества.

Никто не сомневается, что широко используемая группировка десятками объясняется тем, что люди считали на пальцах. Довольно странно, что сохранилось мало свидетельств того, что человек считал на одной руке; пятеричная система встречается исклю-

чительно редко. Но в то же время очень часто встречаются примеры двадцатеричной системы. Не нужно иметь семи пядей во лбу, чтобы понять, что в этой системе в процессе счета участвуют пальцы как рук, так и ног. Из этих двадцатеричных систем счисления, возможно, самая известная — система племени майя, но и в Европе такие системы были широко распространены несколько столетий назад. Двадцатеричная система прослеживается во французском языке в числах от 80 до 100, что можно увидеть из следующих примеров:

80 = quatre-vingts =

= четыре раза по двадцать,

90 = quatre-vingts-dix =

= четыре раза по двадцать и десять

91 = quatre-vingts-onze =

= четыре раза по двадцать и одиннадцать

и так далее.

Менее известно, что в датском языке счет парами десятков процветает вплоть до наших дней. Эта древняя система, которая ранее была широко распространена среди германских племен, столь оригинальна, что мы не можем не привести хотя бы несколько ее деталей.

При счете до 20 естественно использовать такие термины, как:

tredsindstve = три раза по двадцать,

firsindstve = четыре раза по двадцать,

femsindstve = пять раз по двадцать.

Но система становится более сложной, если условиться, что всякий раз, когда мы просчитаем несколько полных двадцаток, а затем еще десяток, объявлять, что находимся на половине следующей двадцатки; например,

90 = halvfemsindstve = половина пятой двадцатки.

Чтобы закончить наше описание, следует сказать, что в датском языке количество единиц ставится пе-

ред количеством десятков, что приводит к числовым конструкциям типа

93 = treoghalvfemsindstyve = три и половина пятой двадцатки.

Ясно, что в любой цивилизации, насыщенной числами, подобно нашей, такие системы обречены. Спотоб записи чисел, при котором единицы ставятся перед десятками, особенно неприятен. Такая система была также распространена в Англии до XVIII века: вместо twenty-three (двадцать три) обычно говорили three and twenty (три и двадцать). В Норвегии лишь несколько лет назад парламент специальным законом отменил использование такой системы в школах и всех официальных сообщениях. Однако подобная система продолжает процветать в Германии, что приводит к многочисленным числовым ошибкам, например, при набирании номера телефона.

С давних времен до наших дней астрономы пользуются древней вавилонской шестидесятеричной системой (с основанием 60). Правда, сейчас ее достоинства уменьшились, но мы все же придерживаемся этой системы при отсчете времени и углов в минутах и секундах. Мы не знаем, почему вавилоняне ввели столь большое основание в свою систему, можно лишь предположить, что эта система возникла как комбинация двух систем с различными основаниями, скажем, 10 и 12, у которых наименьшее общее кратное равно 60.

Теперь скажем несколько слов о математических вопросах, связанных с использованием систем с различными основаниями. При основании b мы записываем целое число

$$N = c_n b^n + c_{n-1} b^{n-1} + \dots + c_2 b^2 + c_1 b + c_0 \quad (6.2.1)$$

так же, как и в (6.1.2), с той разницей, что здесь коэффициенты c_i могут принимать значения

$$c_i = 0, 1, \dots, b-1, \quad (6.2.2)$$

вместо значений, приведенных в (6.1.3). Для краткости можно записать число N из (6.2.1) в сокращенной форме

$$(c_n, c_{n-1}, \dots, c_2, c_1, c_0)_b, \quad (6.2.3)$$

соответствующей записи (6.1.1), при этом в записи (6.2.3) необходимо приписать используемый базис — число b , чтобы избежать путаницы.

Примеры. В шестидесятеричной системе

$$(3, 11, 43)_{60} = 3 \cdot 60^2 + 11 \cdot 60 + 43 = 11\,503.$$

В системе с основанием $b = 4$

$$(3, 2, 0, 1)_4 = 3 \cdot 4^3 + 2 \cdot 4^2 + 0 \cdot 4 + 1 = 225.$$

Вообще, когда число задано в системе с основанием b , мы находим это число в обычной десятичной системе, вычисляя значения степеней числа b , умножая каждое из них на соответствующую цифру и складывая, как уже делалось в вышеприведенных примерах.

Теперь рассмотрим обратную задачу. задается число N и мы хотим представить его при основании b . Мы можем сделать это повторным делением на b . Взгляните на формулу (6.2.1). Можно записать ее в виде

$$N = (c_n b^{n-1} + \dots + c_2 b + c_1) b + c_0.$$

Так как c_0 меньше, чем b , то c_0 является остатком при делении числа N на b . Мы можем записать это деление

$$N = q_1 b + c_0, \quad q_1 = c_n b^{n-1} + \dots + c_2 b + c_1,$$

для того чтобы показать, что c_1 получается делением числа q_1 на b тем же способом, и т. д. Таким образом мы находим коэффициенты c_i в результате серии делений на число b :

$$\begin{aligned} N &= q_1 b + c_0, \\ q_1 &= q_2 b + c_1, \\ &\dots \dots \dots \\ q_{n-1} &= q_n b + c_{n-1}, \\ q_n &= 0 \cdot b + c_n, \end{aligned}$$

при этом мы продолжаем деление до тех пор, пока не окажутся выполненными соотношения $q_n < b$, $q_{n+1} = 0$. Мы приводим два примера, которые помогут вам понять этот процесс.

Пример 1. Выразим число 101 при основании 3. Мы выполняем деление на 3, как указывалось выше, и находим

$$101 = 33 \cdot 3 + 2,$$

$$33 = 11 \cdot 3 + 0,$$

$$11 = 3 \cdot 3 + 2,$$

$$3 = 1 \cdot 3 + 0,$$

$$1 = 0 \cdot 3 + 1.$$

Отсюда

$$101 = (1, 0, 2, 0, 2)_3.$$

Пример 2. Выразим число 1970 при основании 12. Здесь деление на 12 таково:

$$1970 = 164 \cdot 12 + 2,$$

$$164 = 13 \cdot 12 + 8,$$

$$13 = 1 \cdot 12 + 1,$$

$$1 = 0 \cdot 12 + 1.$$

Следовательно,

$$1970 = (1, 1, 8, 2)_{12}.$$

Система задач 6.2.

1. Выразите числа $(1, 2, 3, 4)_5$, $(1, 1, 1, 1, 1)_3$ в десятичной системе.

2. Представьте числа 362, 1969, 10 000 при основаниях $b = 2; 6; 17$.

§ 3. Сравнение систем счисления

Американское общество сторонников двенадцатеричной системы предложило изменить нашу десятиричную систему на более эффективную и удобную, как они думают, систему с основанием 12. Те, кто предлагает эту систему, указывают, что было бы выгоднее иметь систему с основанием, делящимся на числа 2, 3, 4 и 6, так как процесс деления на эти часто встречающиеся делители упрощается. Доводы такого типа привели бы нас к шестидесятеричной системе, основание которой, число 60, делится на числа

2, 3, 4, 5, 6, 10, 12, 15, 20, 30.

В ряде стран многие вещи все еще считают дюжинами и grossами (т. е. дюжинами дюжин) и естественно, что для них двенадцатеричная система является вполне возможной. Для перехода в двенадцатеричную систему нужно было бы ввести двенадцать новых символов, что потребует для их разработки столь же много усилий, сколько потребовалось для создания десятиричной системы. Некоторые энтузиасты считают, что необходимо ввести новые символы лишь для 10 и 11, но такой способ не учитывает неудобств, возникающих в период перехода: никто не будет понимать, например, означает ли запись 325

$$3 \cdot 10^2 + 2 \cdot 10 + 5 = 325$$

или

$$3 \cdot 12^2 + 2 \cdot 12 + 5 = 461.$$

Для того чтобы получить представление о том, как меняется количество знаков в числе в зависимости от системы счисления, возьмем число

$$10^n - 1 = \overbrace{99 \dots 9}^n = N \quad (6.3.1)$$

в десятиричной системе. Это самое большое число с n знаками. Чтобы найти m — количество знаков при записи этого числа при основании b — мы должны определить m как целое число, для которого выполняются неравенства

$$b^m > 10^n - 1 \geq b^{m-1}. \quad (6.3.2)$$

Это условие может быть также записано в виде

$$b^m \geq 10^n > b^{m-1}.$$

Возьмем логарифмы этих трех чисел. Вспомнив, что $\lg 10 = 1$, получим, что

$$m \lg b \geq n > (m-1) \lg b.$$

В свою очередь эти неравенства могут быть переписаны в виде

$$m \geq \frac{n}{\lg b} > m-1; \quad (6.3.3)$$

таким образом, m является первым целым числом не меньшим, чем

$$\frac{n}{\lg b}. \quad (6.3.4)$$

было в действительности редким искусством. Но можно привести и гораздо более поздние примеры.

Самюэль Пепис, известный благодаря своему дневнику, был в возрасте около тридцати лет и служил клерком канцелярии лорда-хранителя печати, когда летом 1662 года он решил, что он должен знать кое-что из математики, по крайней мере основы арифметики, чтобы самостоятельно проверять счета. Заметим, что он тогда уже получил степени бакалавра и магистра в Кембридже. В то время было довольно обычным, что хорошо образованный английский джентльмен совершенно не владеет повседневными расчетами; эти расчеты могли перепоручаться младшим счетоводам.

$$\begin{aligned}
 1 &= \bullet \\
 5 &= \text{—} \\
 6 &= \text{—} \bullet = 1 + 5 \\
 17 &= \text{—} \text{—} \bullet \bullet = 2 + 3 \cdot 5 \\
 137 &= \text{—} \text{—} \text{—} \bullet \bullet = 6 \cdot 20 + 17 = (1 + 5) \cdot 20 + (2 + 3 \cdot 5)
 \end{aligned}$$

Рис. 16.

4 июля 1662 года Пепис записывает в своем дневнике: «Вскоре придет мистер Купер, помощник капитана на „Ройял Чарльз“, у которого я собираюсь учиться математике, и сегодня мы начнем; он очень способный человек, я полагаю, что не найдется дела, которое способно полностью его удовлетворить. После часа занятий арифметикой (я пытался выучить таблицу умножения) мы расстались с ним до завтра».

Каждый день и рано утром и поздно вечером Пепис учил проклятую таблицу умножения, с трудом продвигаясь вперед при поддержке своего моряка-учителя. Например, 9 июля он записывает: «Встал в четыре часа утра и снова упорно учу таблицу умножения, которая для меня является главной трудностью арифметики». Так продолжалось несколько дней, пока 11 июля он смог записать: «Встал в четы-

ре часа утра и упорно работал над таблицей умножения, которой я теперь почти овладел». Пепис хорошо использовал полученные с таким трудом знания на всех все более важных постах, на которые он назначался. Однако может показаться слишком быстрым его продвижение, когда вы узнаете, что он был избран членом знаменитой Британской академии наук — Королевского общества — спустя два с половиной года после того, как выучил таблицу умножения.

Мы привели эту историю, которая никоим образом не является уникальной, чтобы подчеркнуть: запоминание таблицы умножения в те дни не было обычным этапом математического знания. Таким образом, мы видим, что использование в нашей арифметике чисел с небольшим основанием дает ряд преимуществ, как механических, так и интеллектуальных. Например, когда основанием является число $b = 3$, то в таблице умножения

	0	1	2
0,	0	0	0
1	0	1	2
2	0	2	$(1,1)_3$

существует только единственное нетривиальное умножение, а именно:

$$2 \cdot 2 = 4 = (1, 1)_3.$$

Для $b = 2$ мы имеем совершенно тривиальную таблицу

	0	1
0	0	0
1	0	1

Система задач 6.3.

1. Доказать, что количество нетривиальных умножений цифр (получающееся отбрасыванием умножений на 0 и 1) в системе с основанием b равно $\frac{1}{2}(b-1)(b-2)$.

2. Чему равна сумма всех элементов в таблице умножения? Проверьте для $b = 10$.

§ 4. Некоторые задачи, связанные с системами счисления

Обсудим несколько задач, связанных с системами счисления, которые имеют отношение к выбору оснований систем счисления, удобных для машинного счета. Предположим, что мы имеем дело с обычным настольным арифмометром, который работает при помощи сцепленных числовых колес, каждое из которых имеет 10 цифр: 0, 1, ..., 9. Если имеется n колес, то мы можем представить все числа вплоть до

$$N = \overbrace{99 \dots 9}^n, \quad (6.4.1)$$

как и в (6.3.1).

Предположим теперь, что в качестве основания мы взяли число b , отличное от 10, но продолжаем рассматривать числа до N . Тогда мы должны иметь m колес, где m — целое число, удовлетворяющее условиям (6.3.2) и (6.3.3). Как и в (6.3.4), число m является целым числом, равным числу

$$\frac{n}{\lg b}$$

или следующим за ним. Так как каждое колесо несет b цифр, то количество цифр, записанных на колесах, приближенно равно

$$D = n \cdot \frac{b}{\lg b}. \quad (6.4.2)$$

Можно теперь спросить: какое нужно выбрать число b , чтобы получить наименьшее количество чисел, записанных на колесах? Чтобы найти наименьшее значение числа D , в формуле (6.4.2) необходимо лишь исследовать функцию

$$f(b) = \frac{b}{\lg b} \quad (6.4.3)$$

для различных оснований $b = 2, 3, 4, \dots$. С помощью таблицы логарифмов получаем значения

b	2	3	4	5	6
$f(b)$	6,64	6,29	6,64	7,15	7,71

Последующие значения для $f(b)$ еще больше; например, $f(10)=10$, как уже отмечалось. Мы заключаем, что для таких арифмометров имеет место следующее утверждение.

Наименьшее общее число цифр на арифмометре достигается при $b=3$.

Видно, что для $b=2$ и $b=4$ общее число цифр не на много больше; в этом смысле маленькие основания имеют преимущество.

Рассмотрим небольшое изменение этой задачи. Обычные счеты того типа, который иногда используется для обучения детей счету, имеют несколько металлических спиц с девятью *) подвижными косточками на каждой из них, чтобы отмечать цифры чисел. С таким же успехом можно провести параллельные прямые на листе бумаги и отмечать цифры соответствующим количеством спичек, или же подобно древним начертить эти прямые на песке и отмечать цифры камешками.

Но вернемся к счетам. Если имеется n спиц и на каждой по 9 косточек, то можно представить вновь все целые числа с n знаками вплоть до числа N , записанного в (6.4.1). Теперь зададим следующий вопрос: можно ли, взяв другое основание b , сделать счеты более компактными, т. е. обойтись меньшим количеством косточек?

При основании b количество косточек на каждой спице будет $b-1$. Как и прежде, для того чтобы счеты имели ту же вместимость N , количество знаков или спиц должно определяться соотношением (6.3.4). Это дает значение

$$E = \frac{n}{\lg b} (b - 1) \quad (6.4.4)$$

в качестве приближения для общего количества косточек. Чтобы найти, когда это число принимает наименьшее возможное значение, мы должны исследовать функцию

$$g(b) = \frac{b-1}{\lg b} \quad (6.4.5)$$

*) На счетах, принятых в СССР, на каждой спице располагается 10 косточек. (Прим. перев.)

для различных значений числа $b = 2, 3, \dots$. Значение функции $g(b)$ для небольших значений числа b даны в таблице

b	2	3	4	5	6
$g(b)$	3,32	4,19	4,98	5,72	6,43

Для больших значений числа b функция продолжает возрастать, поэтому мы заключаем, что

необходимое количество косточек на счетах будет минимально при $b = 2$.

Можно интерпретировать этот результат с другой точки зрения. Предположим, что мы отметили цифры нашего числа, используя спички или камешки, расположенные на прямых линиях. В десятичной системе будет от 0 до 9 отметок на каждой прямой. Это дает в среднем по 4,5 спички на каждой прямой для наугад взятых чисел; следовательно, числа с n знаками потребуют в среднем 4,5 n спичек, когда они укладываются произвольно.

Посмотрим, какое время потребуется, чтобы уложить эти спички на места. Имея в виду какое-нибудь расположение, предположим, что потребуется одна секунда, чтобы уложить одну спичку. Тогда общее время, требуемое для того, чтобы уложить все спички, будет в среднем составлять приблизительно 4,5 n секунд.

Предположим, что мы изменили наше основание на число b и допустим ту же самую вместимость для представления чисел. В таком случае на каждой прямой будет от 0 до $b - 1$ спичек, следовательно, в среднем

$$\frac{1}{2}(b - 1)$$

из всего количества спичек. Как мы упоминали несколько раз, мы будем иметь приблизительно

$$\frac{n}{\lg b}$$

прямых. Отсюда делаем вывод, что среднее время, требуемое для представления числа с n знаками, со-

ставляет примерно

$$\frac{n}{\lg b} \cdot \frac{1}{2} (b - 1) = \frac{1}{2} E$$

секунд, здесь E есть выражение из (6.4.4). Так как это время было минимальным для $b = 2$, мы также можем сделать вывод:

среднее время, необходимое для установления числа с помощью спичек на прямых, минимально для $b = 2$.

Система задач 6.4.

1. Постройте графики функций $y = f(b)$ из (6.4.3) и $y = g(b)$ из (6.4.5) для $b > 1$. Если вы уже знакомы с дифференциальным исчислением, используйте его для определения формы кривых.

§ 5. Компьютеры и их системы счисления

До появления электронных вычислительных машин всюду при вычислениях безраздельно господствовала десятичная система. Интерес к другим системам носил либо исторический, либо познавательный характер. Существовало лишь несколько отдельных задач, которые наиболее удачно формулировались с использованием двоичной или троичной систем счисления. Одним из излюбленных примеров в книгах по теории чисел является игра «Ним» *). К тому времени, когда появилось много различных типов компьютеров, возникла задача сделать устройство ЭВМ как можно более компактным и эффективным. Это привело к тщательному изучению систем счисления с целью нахождения более подходящей системы. По ряду причин, некоторые из которых мы обсудили в предыдущем параграфе, двоичная система была признана предпочтительной. Единственным ее недостатком явилось то, что для большинства из нас требуются немалые усилия для того, чтобы чув-

*) При игре в «Ним» раскладывается некоторое количество камешков в несколько кучек. Двое играющих по очереди берут камешки из кучек, при ходе можно брать произвольное количество камней, но только из одной кучки. Выигрывает игрок, взявший последний камень. (Прим. перев.)

ствовать себя в ней «как дома», так как мы были воспитаны в других традициях. Следовательно, поскольку числа, которые должны вводиться в компьютеры, обычно записаны в десятичной системе, то требуется начальное устройство, переводящее их в двоичную систему, а ответы в конце концов должны быть выражены в десятичной системе, как уступка менее математически подготовленным членам общества.

Разумеется, двоичная система, используемая в ЭВМ, является той же самой системой, которую мы обсуждали в предыдущем параграфе, однако используемая терминология носит более технический оттенок. Двоичные цифры 0, 1 называются *битами*, что является сокращением английского выражения Binary digiTs (двоичные цифры). Так как существуют лишь две возможности: 0 и 1 в каждой позиции, то часто говорят об элементе с двумя состояниями.

Если следовать общему правилу, изложенному в § 2 этой главы, то представление данного числа в двоичной системе довольно просто. Например, возмем $N = 1971$. Повторное деление на $b = 2$ дает

$$1971 = 985 \cdot 2 + 1,$$

$$985 = 492 \cdot 2 + 1.$$

$$492 = 246 \cdot 2 + 0,$$

$$246 = 123 \cdot 2 + 0,$$

$$123 = 61 \cdot 2 + 1,$$

$$61 = 30 \cdot 2 + 1,$$

$$30 = 15 \cdot 2 + 0,$$

$$15 = 7 \cdot 2 + 1,$$

$$7 = 3 \cdot 2 + 1,$$

$$3 = 1 \cdot 2 + 1,$$

$$1 = 0 \cdot 2 + 1,$$

Следовательно,

$$1971_{10} = (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)_2.$$

Ранее мы отмечали, что в двоичной системе числа имеют более длинные выражения, следовательно, становится труднее с первого взгляда оценить величину

числа. По этой причине в языке ЭВМ часто используется восьмеричная система счисления (с основанием 8). Это является лишь незначительным изменением двоичной системы, которое получается разбиением бит в числе на группы по три. Это можно представить себе как систему с основанием

$$b = 8 = 2^3.$$

Коэффициентами при этом являются восемь чисел

$$0 = 000, \quad 4 = 100,$$

$$1 = 001, \quad 5 = 101,$$

$$2 = 010, \quad 6 = 110,$$

$$3 = 011, \quad 7 = 111.$$

В качестве иллюстрации возьмем число 1971 из рассмотренного выше примера; в восьмеричной системе оно представляется как

$$1971 = 011, 110, 110, 011 = (3, 6, 6, 3)_8.$$

Таким образом, этот способ записи незначительно отличается от предыдущего. В действительности, такое деление на группы нам хорошо знакомо по обычным десятичным числам: при записи и произнесении большого числа мы обычно делим его цифры на группы по три, например,

$$N = 89\,747\,321\,924.$$

Таким образом, можно сказать, что это является представлением нашего числа при основании

$$b = 1000 = 10^3.$$

В компьютерах иногда используются и другие представления чисел. Предположим, что мы хотим записать десятичное число, скажем, $N = 2947$, в ЭВМ, работающей в двоичной системе. Тогда, вместо того чтобы полностью менять N на двоичное число, можно было бы изменить лишь цифры этого числа

$$2 = 0010,$$

$$9 = 1001,$$

$$4 = 0100,$$

$$7 = 0111$$

и, таким образом,

$$N = 0010, 1001, 0100, 0111.$$

Такие числа известны как *кодированные десятичные числа*. Этот метод иногда называется «системой 8421», так как эти десятичные цифры представляются в виде сумм двоичных единиц

$$0 = 0000, \quad 1 = 0001, \quad 2 = 0010,$$

$$2^2 = 4 = 0100, \quad 2^3 = 8 = 1000.$$

Такие кодированные десятичные числа неудобны для всех видов вычислений, но не всегда целью ЭВМ являются вычисления. Тем же образом, любая буква алфавита или любой другой символ могут быть написаны какому-нибудь двоичному числу. Это означает, что любое слово или предложение можно запоминать как двоичное число. Таким образом, если бы мы были соответствующим образом натренированы и имели бы дело со столь же подготовленной аудиторией, то могли бы общаться лишь с помощью бит.

Система задач 6.5.

1. Найдите двоичное представление чисел Ферма (§ 3, гл. 2)

$$F_t = 2^{2^t} + 1.$$

2. Найдите двоичные представления четных совершенных чисел (§ 4, гл. 3)

$$P = 2^{p-1}(2^p - 1).$$

§ 6. Игры с числами

Существует множество видов игр с числами, некоторые из которых были известны еще в средние века. Большинство из них не представляет интереса для теории чисел, скорее всего, они подобно магическим квадратам принадлежат к классу кроссвордов с числами. Некоторые из них проиллюстрируем примерами.

Перед вами телеграмма, посланная школьником домой, с настоятельной просьбой:

$$\begin{array}{r} S \ E \ N \ D \\ M \ O \ R \ E \\ \hline M \ O \ N \ E \ Y^*) \end{array}$$

Будем рассматривать эту схему, как сложение двух четырехзначных чисел SEND и MORE, в сумме дающих число MONEY. Каждая буква означает определенную цифру. Задача состоит в том, чтобы определить, какие это цифры. Так как всего 10 цифр, то в каждой такой задаче может фигурировать не более 10 букв, в этом примере 8. В идеальном случае задача должна иметь единственное решение.

В нашем примере очевидно, что

$$M = 1,$$

так как M — первая цифра либо суммы $S + M$, либо $S + M + 1$, где S и M — числа, не превосходящие числа 9. Тогда для числа S имеются две возможности:

$$S = 9 \quad \text{или} \quad S = 8,$$

так как либо $S + 1$, либо $S + 1 + 1$ есть двузначное число. Установим сначала, что S не может быть цифрой 8, ибо, если бы S было 8, то должен был бы быть перенос из колонки сотен, что дает

$$S + M + 1 = 8 + 1 + 1 = 10$$

при сложении в колонке сотен. Следовательно, O должно было бы быть нулем и наше послание читалось бы так:

$$\begin{array}{r} 8 \ E \ N \ D \\ 1 \ 0 \ R \ E \\ \hline 1 \ 0 \ N \ E \ Y \end{array}$$

Но, исследуя колонку сотен, находим, что обязательно должен быть перенос из колонки десятков (иначе $E + 0 = E$, а не N), и так как $E \leq 9$, то

$$E + 0 + 1 = 10.$$

Это вынудило бы нас положить $N = 0$, но мы уже знаем, что $O = 0$, поэтому такой случай невозможен,

*) Вышлите побольше денег.

и мы заключаем, что $S = 9$, и послание теперь читается так:

$$\begin{array}{rcccc} 9 & E & N & D \\ 1 & 0 & R & E \\ \hline 1 & 0 & N & E & Y \end{array}$$

Так как $E \neq N$, то сложение в колонке сотен приводит к условию

$$E + 1 = N,$$

и

$$\begin{array}{rcccc} 9 & E & E + 1 & D \\ 1 & 0 & R & E \\ \hline 1 & 0 & E + 1 & E & Y \end{array}$$

Сложение в колонке десятков дает либо

$$E + 1 + R = 10 + E, \text{ либо } E + 1 + R + 1 = 10 + E.$$

Первый случай невозможен, так как он дает $R = 9$, что противоречит тому, что $S = 9$. Во втором случае

$$R = 8,$$

и послание читается так:

$$\begin{array}{rcccc} 9 & E & E + 1 & D \\ 1 & 0 & 8 & E \\ \hline 1 & 0 & E + 1 & E & Y \end{array}$$

И наконец, сумма в колонке единиц такова:

$$D + E = 10 + Y.$$

Для трех букв D , E , Y остаются только значения 2, 3, 4, 5, 6, 7. Наибольшая сумма двух различных чисел из них равна 13. Отсюда существует всего две возможности для Y : либо $Y = 2$, либо $Y = 3$. Последний случай невозможен, так как при этом $D + E = 13$, но мы не можем иметь $E = 7$, так как тогда $N = E + 1 = 8 = R$; также не может быть $D = 7$, так как тогда $E = 6$ и

$$N = E + 1 = 7 = D.$$

Таким образом, $Y = 2$ и $D + E = 12$. Из имеющихся цифр 2, 3, 4, 5, 6, 7 единственной парой, в сумме

дающей 12, являются 5 и 7. Так как $E \neq 7$, то это означает, что $D=7$, $E=5$ и, таким образом, единственное решение нашей задачи следующее:

$$\begin{array}{r} 9 \ 5 \ 6 \ 7 \\ 1 \ 0 \ 8 \ 5 \\ \hline 10 \ 6 \ 5 \ 2 \end{array}$$

Этот процесс довольно сложен, во многих случаях можно получить решение гораздо более простым путем.

Система задач 6.6.

1. Попробуйте проанализировать следующие примеры только что показанным методом:

$$\begin{array}{r} 1. \quad S \ E \ N \ D \\ \quad M \ O \ R \ E \\ \quad G \ O \ L \ D \\ \hline M \ O \ N \ E \ Y \end{array} \quad \begin{array}{r} 2. \quad H \ O \ C \ U \ S \\ \quad P \ O \ C \ U \ S \\ \hline P \ R \ E \ S \ T \ O \end{array}$$

$$\begin{array}{r} 3. \quad F \ O \ R \ T \ Y \\ \quad \quad T \ E \ N \\ \quad \quad T \ E \ N \\ \hline S \ I \ X \ T \ Y \end{array}$$

$$\begin{array}{r} 4. \quad A \ D \ A \ M \\ \quad A \ N \ D \\ \quad E \ V \ E \\ \quad \quad A \\ \hline R \ A \ F \ T \end{array} \quad \begin{array}{r} 5. \quad S \ E \ E \\ \quad S \ E \ E \\ \quad S \ E \ E \\ \quad Y \ E \ S \\ \hline E \ A \ S \ Y \end{array}$$

Переводы этих ребусов таковы:

1. «Шлите больше золотых монет», 2. «Фокус — Покус — Престо», 3. «Сорок + десять + десять = шестьдесят», 4. «Адам и Ева на плоту», 5. «Смотри, смотри, смотри. Да! Легко».

Если хотите, попробуйте придумать свои ребусы. Если вы знакомы с ЭВМ, то попробуйте запрограммировать решение таких задач.

СРАВНЕНИЯ

§ 1. Определение сравнения

Теория чисел имеет свою алгебру, известную, как *теория сравнений*. Обычная алгебра первоначально развивалась как стенография для операций арифметики. Аналогично, сравнения представляют собой символический язык для делимости, основного понятия теории чисел. Понятие сравнения впервые ввел Гаусс.

Прежде чем мы обратимся к понятию сравнения, сделаем одно замечание о числах, которые будем изучать в этой главе. Мы начали эту книгу, заявив, что будем рассматривать целые положительные числа 1, 2, 3, ..., и в предыдущих главах мы ограничивались только этими числами и дополнительным числом 0. Но теперь мы достигли стадии, на которой целесообразно расширить наши границы, рассматривая все целые числа:

$$0, \pm 1, \pm 2, \pm 3, \dots$$

Это никоим образом не повлияет на наши предыдущие понятия; далее, когда мы будем говорить о простых числах, делителях, наибольших общих делителях и тому подобном, мы будем считать их целыми положительными числами.

Теперь вернемся к языку сравнений. Если a и b — два целых числа и их разность $a - b$ делится на число m , мы выражаем это записью

$$a \equiv b \pmod{m}, \quad (7.1.1)$$

которая читается так:

a сравнимо с b по модулю m .

Делитель m мы предполагаем положительным; он называется *модулем сравнения*. Наше высказывание

(7.1.1) означает, что

$$a - b = mk, \text{ где } k \text{ — целое число.} \quad (7.1.2)$$

Примеры.

- 1) $23 \equiv 8 \pmod{5}$, так как $23 - 8 = 15 = 5 \cdot 3$;
- 2) $47 \equiv 11 \pmod{9}$, так как $47 - 11 = 36 = 9 \cdot 4$;
- 3) $-11 \equiv 5 \pmod{8}$, так как $-11 - 5 = -16 = 8 \cdot (-2)$;
- 4) $81 \equiv 0 \pmod{27}$, так как $81 - 0 = 81 = 27 \cdot 3$.

Последний пример показывает, что вообще, вместо того, чтобы говорить: число a делится на число m , мы можем записать

$$a \equiv 0 \pmod{m},$$

так как это означает, что

$$a - 0 = a = mk,$$

где k — некоторое целое число. Например, вместо того, чтобы сказать, что a — четное число, мы можем записать

$$a \equiv 0 \pmod{2}.$$

Таким же образом видно, что нечетное число является числом, удовлетворяющим сравнению

$$a \equiv 1 \pmod{2}.$$

Эта несколько странная терминология является довольно обычной для математических работ.

§ 2. Некоторые свойства сравнений

Способ, которым мы записываем сравнения, напоминает нам уравнения, и в действительности, сравнения и алгебраические уравнения имеют много общих свойств. Простейшими из них являются три следующих свойства:

$$a \equiv a \pmod{m}; \quad (7.2.1)$$

это является следствием того, что

$$a - a = m \cdot 0,$$

$$a \equiv b \pmod{m} \text{ означает, что и } b \equiv a \pmod{m}. \quad (7.2.2)$$

Это следует из того, что $b - a = -(a - b) = m(-k)$.

Из

$$a \equiv b \pmod{m} \quad \text{и} \quad b \equiv c \pmod{m} \quad (7.2.3)$$

следует, что $a \equiv c \pmod{m}$, потому что первые два утверждения означают, что

$$a - b = mk, \quad b - c = ml,$$

поэтому

$$a - c = (a - b) + (b - c) = m(k + l).$$

Пример. Из того, что

$$13 \equiv 35 \pmod{11} \quad \text{и} \quad 35 \equiv -9 \pmod{11}$$

следует, что

$$13 \equiv -9 \pmod{11}.$$

Мы говорили, что сравнения похожи по своему свойству на равенства. В действительности, мы можем рассматривать равенства как тип сравнения, а именно, сравнения по модулю 0. По определению,

$$a \equiv b \pmod{0}$$

означает, что

$$a - b = 0 \cdot k = 0$$

или

$$a = b.$$

Вы почти никогда не встретите такую форму сравнения для записи уравнений в математической литературе. Но существует другое сравнение, очевидно, довольно тривиальное, которое иногда используется. Когда модуль есть число $m = 1$, мы имеем, что

$$a \equiv b \pmod{1} \quad (7.2.4)$$

для любой пары целых чисел a и b , так как это означает, что

$$a - b = 1 \cdot k = k \quad (7.2.5)$$

есть целое число. Но предположим теперь на мгновение, что a и b — произвольные вещественные числа, необязательно целые. Тогда тот факт, что они сравнимы по модулю 1, означает, что их разность есть целое число, т. е. эти два числа имеют одинаковую дробную часть.

Пример. $8\frac{1}{3} \equiv 1\frac{1}{3} \pmod{1}$, или

$$8,333 \dots \equiv 1,333 \dots \pmod{1}.$$

Вернемся к свойствам обычных сравнений целых чисел; с этого момента мы будем всегда считать, что модуль является целым числом $m \geq 2$.

Мы можем разделить числовую ось, начиная от начала координат в обоих направлениях на отрезки длиной m , как на рис. 17. Тогда каждое целое число a , положительное или отрицательное, попадает на

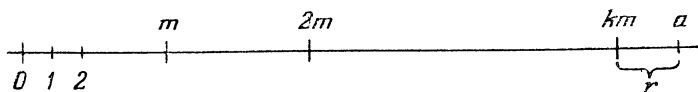


Рис. 17.

один из этих отрезков или на одну из точек деления; таким образом, мы можем записать

$$a = km + r, \quad (7.2.6)$$

где k — некоторое целое число, а r — одно из чисел

$$0, 1, 2, \dots, m-1. \quad (7.2.7)$$

Это является незначительным обобщением деления положительных чисел, описанного в § 3 главы 4. Здесь мы также называем число r в формуле (7.2.6) *остатком* при делении числа a на число m или *остатком по модулю m* .

Примеры.

$$1) \ a = 11, \quad m = 7, \quad 11 = 7 \cdot 1 + 4,$$

$$2) \ a = -11, \quad m = 7, \quad -11 = 7(-2) + 3.$$

Деление (7.2.6) может быть также записано как сравнение

$$a \equiv r \pmod{m}. \quad (7.2.8)$$

Таким образом, каждое число сравнимо со своим остатком по модулю m . В приведенных выше примерах мы имеем

$$11 \equiv 4 \pmod{7}, \quad -11 \equiv 3 \pmod{7}.$$

Никакие два остатка в (7.2.7) не сравнимы по \pmod{m} , так как разность между любыми двумя из них меньше, чем m . Поэтому два числа, которые не

сравнимы по $(\text{mod } m)$, должны иметь разные остатки. Итак, мы делаем вывод:

сравнение $a \equiv b \pmod{m}$ выполняется тогда и только тогда, когда числа a и b имеют одинаковые остатки при делении на число m .

Существует другой способ представления этого сравнения. Предположим на мгновение, что a и b — целые положительные числа. Мы видели при обсуждении системы чисел в § 2 главы 6, что когда число a записано при основании m ,

$$a = (a_n, \dots, a_1, a_0)_m,$$

то последняя цифра a_0 является остатком числа a при делении его на число m . Если мы используем этот факт, чтобы иначе выразить нашу интерпретацию сравнения, то можно сказать:

сравнение $a \equiv b \pmod{m}$ выполняется для целых (положительных) чисел a и b тогда и только тогда, когда числа a и b имеют одинаковые последние цифры в записи при основании m .

Например,

$$37 \equiv 87 \pmod{10},$$

так как эти два числа имеют одну и ту же последнюю цифру в десятичной системе чисел.

Система задач 7.2.

1. Найдите остатки $-37 \pmod{7}$, $-111 \pmod{11}$, $-365 \pmod{30}$.

§ 3. Алгебра сравнений

Из алгебры мы помним, что уравнения можно складывать, вычитать, умножать. Точно такие же правила справедливы для сравнений. Предположим, что мы имеем сравнения

$$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m}. \quad (7.3.1)$$

По определению, это означает, что

$$a = b + mk, \quad c = d + ml, \quad (7.3.2)$$

где k и l — целые числа. Сложим уравнения (7.3.2). В результате получаем

$$a + c = b + d + m(k + l),$$

что можем записать как

$$a + c \equiv b + d \pmod{m}; \quad (7.3.3)$$

другими словами, два сравнения можно складывать. Таким же образом можно показать, что одно сравнение можно вычитать из другого, т. е. что

$$a - c \equiv b - d \pmod{m}. \quad (7.3.4)$$

Пример.

$$11 \equiv -5 \pmod{8} \quad \text{и} \quad 7 \equiv -9 \pmod{8}. \quad (7.3.5)$$

Складывая их, получаем

$$18 \equiv -14 \pmod{8},$$

а вычитая,

$$4 \equiv 4 \pmod{8}.$$

Оба эти сравнения справедливы.

Можно также перемножить два сравнения. Из (7.3.1) и (7.3.2) следует, что

$$ac = bd + m(kd + bl + mkl),$$

таким образом,

$$ac \equiv bd \pmod{m}. \quad (7.3.6)$$

Пример. Когда два сравнения из (7.3.5) перемножены, получается

$$77 \equiv 45 \pmod{8}.$$

Сравнение $a \equiv b \pmod{m}$ может быть умножено на любое целое число c , при этом получаем

$$ac \equiv bc \pmod{m}. \quad (7.3.7)$$

Это можно рассматривать как частный случай умножения сравнений (7.3.6) при $c = d$. Его можно также рассматривать как прямое следствие из определения сравнения.

Пример. Когда первое сравнение из (7.3.5) умножается на 3, получаем, что

$$33 \equiv -15 \pmod{8}.$$

Возникает естественный вопрос: в каком случае можно в сравнении (7.3.7) сократить общий множитель c и получить при этом верное сравнение

$$a \equiv b \pmod{m}?$$

Именно здесь сравнения отличаются от уравнений. Например, верно, что

$$22 \equiv -2 \pmod{8},$$

но сокращение на множитель 2 дало бы сравнение

$$11 \equiv -1 \pmod{8},$$

которое неверно.

В одном важном случае сокращение допустимо: *если $ac \equiv bc \pmod{m}$, то $a \equiv b \pmod{m}$ при условии, что числа m и c взаимно просты.*

Доказательство. Первое сравнение означает, что

$$ac - bc = (a - b)c = mk.$$

Если $D(m, c) = 1$, то отсюда следует, что $a - b$ делится на m в соответствии с результатом, доказанным в § 2 главы 4.

Пример. В сравнении

$$4 \equiv 48 \pmod{11}$$

мы можем сократить на множитель 4, так как $D(11, 4) = 1$. Это дает

$$1 \equiv 12 \pmod{11}.$$

Система задач 7.3.

1. Придумайте еще несколько примеров на использование изложенных правил действий со сравнениями.

§ 4. Возведение сравнений в степень

Предположим вновь, что имеется сравнение

$$a \equiv b \pmod{m}.$$

Как мы только что видели, можно умножить это сравнение на себя, получив

$$a^2 \equiv b^2 \pmod{m}.$$

Вообще можно, умножив это сравнение на себя нужное количество раз, получить

$$a^n \equiv b^n \pmod{m}$$

для любого целого положительного числа n .

Пример. Из сравнения

$$8 \equiv -3 \pmod{11}$$

после возведения в квадрат следует сравнение

$$64 \equiv 9 \pmod{11},$$

а после возведения в куб получаем сравнение

$$512 \equiv -27 \pmod{11}.$$

Многие результаты теории сравнений связаны с остатками высоких степеней чисел, поэтому покажем, как можно продолжить процесс возведения в степень. Предположим, например, что мы хотим найти остаток сравнения

$$3^{89} \pmod{7}.$$

Одним из путей для выполнения этого является повторное возведение в квадрат. Мы находим:

$$9 = 3^2 \equiv 2 \pmod{7},$$

$$3^4 \equiv 4,$$

$$3^8 \equiv 16 \equiv 2,$$

$$3^{16} \equiv 4,$$

$$3^{32} \equiv 16 \equiv 2,$$

$$3^{64} \equiv 4 \pmod{7}.$$

Так как

$$89 = 64 + 16 + 8 + 1 = 2^6 + 2^4 + 2^3 + 1,$$

то отсюда следует, что

$$3^{89} = 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3 = 4 \cdot 4 \cdot 2 \cdot 3 \equiv 5 \pmod{7}.$$

Таким образом, остаток (по модулю 7) есть 5, или, говоря другими словами, в соответствии с изложенным в § 2, последняя цифра числа 3^{89} , записанного в системе счисления при основании 7, равна 5.

В действительности, для того чтобы найти этот остаток, мы записали показатель степени

$$89 = 2^6 + 2^4 + 2^3 + 1 = (1, 0, 1, 1, 0, 0, 1)_2$$

в двоичной системе счисления. Повторным возведением в квадрат мы нашли остатки (по модулю 7)

тех степеней числа 89, которые сами являются степенями числа 2:

$$1, 2, 4, 8, 16, 32, 64.$$

Соответствующий метод можно использовать для любых других оснований. Однако в частном случае бывает возможность упростить вычисление, если заметить особенности этого случая. Например, в случае, разобранном выше, мы можем отметить, что

$$3^3 \equiv -1 \pmod{7},$$

$$3^6 \equiv 1 \pmod{7},$$

откуда заключаем, что

$$3^{84} = (3^6)^{14} \equiv 1 \pmod{7}.$$

Поэтому

$$3^{89} = 3^{84} \cdot 3^3 \cdot 3^2 \equiv 1 \cdot (-1) \cdot 2 = -2 \equiv 5 \pmod{7},$$

как и раньше.

В качестве другой иллюстрации сказанного можно рассмотреть числа Ферма, с которыми мы познакомились в § 3 гл. 2:

$$F_t = 2^{2^t} + 1.$$

Первые пять чисел Ферма таковы:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Отсюда можно высказать предположение:

десятичная запись всех чисел Ферма, за исключением F_0 и F_1 , оканчивается цифрой 7.

Докажем с помощью сравнений, что это действительно так. Очевидно, что оно равносильно утверждению, что числа

$$2^{2^t}, \quad t = 2, 3, \dots$$

оканчиваются цифрой 6. Это можно доказать по индукции. Заметим, что

$$2^{2^2} = 16 \equiv 6 \pmod{10},$$

$$2^{2^3} = 256 \equiv 6 \pmod{10},$$

$$2^{2^4} = 65536 \equiv 6 \pmod{10}.$$

Более того, если мы возводим в квадрат число 2^{2^k} , то результатом будет число

$$(2^{2^k})^2 = 2^{2 \cdot 2^k} = 2^{2^{k+1}}.$$

Предположим, что для некоторого значения t

$$2^{2^t} \equiv 6 \pmod{10};$$

возводя в квадрат это сравнение, мы находим, что

$$2^{2^{t+1}} \equiv 36 \equiv 6 \pmod{10},$$

что и требовалось.

§ 5. Теорема Ферма

Из алгебры мы знаем правила возведения бинома в степень:

$$\begin{aligned}(x+y)^1 &= x+y, \\(x+y)^2 &= x^2+2xy+y^2, \\(x+y)^3 &= x^3+3x^2y+3xy^2+y^3, \\(x+y)^4 &= x^4+4x^3y+6x^2y^2+4xy^3+y^4\end{aligned}\tag{7.5.1}$$

и вообще

$$(x+y)^p = x^p + C_p^1 x^{p-1}y + C_p^2 x^{p-2}y^2 + \dots + y^p. \tag{7.5.2}$$

Здесь первый и последний коэффициенты равны единице. Средними биномиальными коэффициентами являются

$$C_p^1 = \frac{p}{1}, \quad C_p^2 = \frac{p(p-1)}{1 \cdot 2}, \quad C_p^3 = \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3}, \dots \tag{7.5.3}$$

и вообще

$$C_p^r = \frac{p(p-1)(p-2)\dots(p-r+1)}{1 \cdot 2 \dots r}, \tag{7.5.4}$$

где

$$r = 1, 2, \dots, p-1.$$

Так как эти коэффициенты получаются в результате последовательного умножения на бином $(x+y)$, то ясно, что они являются целыми числами.

С этого момента будем считать, что p — простое число. Чтобы записать эти коэффициенты в целочис-

ленном виде, необходимо сократить все общие множители знаменателя

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot r$$

и числителя

$$p(p-1) \dots (p-r+1).$$

Однако знаменатель не содержит простого множителя p , поэтому после сокращения число p останется множителем в числителе. Мы делаем вывод.

Все биномиальные коэффициенты (кроме первого и последнего) в выражении (7.5.2) делятся на p , если p — простое число.

Пусть теперь x и y в выражении (7.5.2) будут целыми числами. Если мы рассмотрим формулу (7.5.2) как сравнение по модулю p , то можно сделать вывод, что для любых целых чисел x и y и простого p

$$(x+y)^p \equiv x^p + y^p \pmod{p}. \quad (7.5.5)$$

В качестве примера возьмем $p = 5$:

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5.$$

Так как все средние коэффициенты делятся на 5, то

$$(x+y)^5 \equiv x^5 + y^5 \pmod{5}$$

в соответствии с (7.5.5).

Из сравнения (7.5.5) можно сделать важные выводы. Применим его для случая $x = y = 1$. Получаем

$$2^p = (1+1)^p \equiv 1^p + 1^p = 2 \pmod{p}.$$

Возьмем затем $x = 2, y = 1$ и найдем, что

$$3^p = (2+1)^p \equiv 2^p + 1^p;$$

теперь, используя предыдущий результат, $2^p \equiv 2 \pmod{p}$, получаем

$$2^p + 1^p \equiv 2 + 1 \equiv 3 \pmod{p}.$$

Итак, $3^p \equiv 3 \pmod{p}$. Далее для $x = 3, y = 1$ получаем

$$4^p \equiv 4 \pmod{p}.$$

Используя этот процесс, можно доказать по индукции, что $a^p \equiv a \pmod{p}$ для всех значений числа

$$a = 0, 1, \dots, p-1. \quad (7.5.6)$$

Случаи $a = 0$ и $a = 1$ очевидны. Так как каждое число сравнимо $(\text{mod } p)$ с одним из остатков, записанных в (7.5.6), мы делаем вывод:

для любого целого числа a и любого простого числа p

$$a^p \equiv a \pmod{p}. \quad (7.5.7)$$

Это утверждение обычно называют *теоремой Ферма*, хотя некоторые авторы называют ее *малой теоремой Ферма*, чтобы отличить от последней теоремы Ферма, или гипотезы Ферма, о которой мы упоминали в § 3 главы 5.

Пример. Для $p = 13$ и $a = 2$ мы находим: $13 = 8 + 4 + 1$, т. е. $2^{13} = 2^{8+4+1} = 2^8 \cdot 2^4 \cdot 2^1$. Так как

$$2^4 = 16 \equiv 3 \pmod{13}, \quad 2^8 \equiv 9 \pmod{13},$$

то

$$2^{13} = 2^8 \cdot 2^4 \cdot 2 \equiv 9 \cdot 3 \cdot 2 \equiv 2 \pmod{13},$$

как и утверждает теорема Ферма.

В соответствии с правилом сокращения для сравнений, сформулированным в конце § 3, мы можем сократить общий множитель a в обеих частях записи теоремы Ферма (7.5.7) при условии, что число a взаимно просто с числом p , являющимся модулем сравнения. Это дает следующий результат:

если a является целым числом, не делящимся на простое число p , то

$$a^{p-1} \equiv 1 \pmod{p}. \quad (7.5.8)$$

Этот результат также называют *теоремой Ферма*.

Пример. Когда $a = 7$, $p = 19$, мы находим, что

$$7^2 = 49 \equiv 11 \pmod{19}$$

$$7^4 = 121 \equiv 7 \pmod{19},$$

$$7^8 = 49 \equiv 11 \pmod{19},$$

$$7^{16} = 121 \equiv 7 \pmod{19},$$

и это дает

$$a^{p-1} = 7^{18} = 7^{16} \cdot 7^2 \equiv 7 \cdot 11 \equiv 1 \pmod{19},$$

что соответствует утверждению (7.5.8).

В качестве приложения теоремы Ферма вновь рассмотрим треугольники Пифагора, обсужденные в гл. 5 и докажем следующее утверждение:

произведение длин сторон треугольника Пифагора делится на 60.

Доказательство. Очевидно, достаточно доказать это для простейших треугольников. В соответствии с формулой (5.2.7), это произведение есть

$$P = 2mn(m^2 - n^2)(m^2 + n^2) = 2mn(m^4 - n^4).$$

Число P делится на 60 тогда и только тогда, когда оно делится на 4, на 3 и на 5. Так как одно из чисел m и n четно, то $2mn$, а следовательно, и число P , делится на 4. Оно делится на 3, если хотя бы одно из чисел m или n делится на 3, но если ни одно из них не делится на 3, то P все же будет делиться на 3, так как из условий (7.5.8), а также $D(m, 3) = 1$ и $D(n, 3) = 1$ следует, что $m^2 \equiv 1 \pmod{3}$ и $n^2 \equiv 1 \pmod{3}$, так что

$$m^2 - n^2 \equiv 1 - 1 \equiv 0 \pmod{3}.$$

Аналогично, число P делится на 5. Это очевидно, если m или n делится на 5. Если ни одно из них не делится на 5, то вновь по теореме Ферма (7.5.8) получаем

$$m^4 - n^4 \equiv 1 - 1 \equiv 0 \pmod{5}.$$

НЕКОТОРЫЕ ПРИМЕНЕНИЯ СРАВНЕНИЙ

§ 1. Проверка вычислений

Как мы уже упоминали, создателем теории сравнений был немецкий математик Карл Фридрих Гаусс. Его знаменитая работа по теории чисел «Арифметические исследования» появилась в 1801 году, когда ему было 24 года. В первых главах этой книги рассказывается о теории сравнений. Однако здесь следует упомянуть, что следы теории сравнений можно обнаружить за несколько столетий до Гаусса. Некоторые из них присутствуют в древних правилах проверки арифметических вычислений. Они составляют существенную часть инструкции по арифметическим операциям эпохи Ренессанса. Некоторые из них используются до сих пор, а из всего того, что нам известно об их происхождении, можно сказать, что их корни лежат в античности.

Мы не знаем, каким образом эти правила были впервые введены, однако попытаемся указать один из возможных путей, на котором они могли быть открыты. Вернемся к временам счетных досок. На таком абаке каждая цифра в числах, которые участвовали в вычислениях, обычно выкладывалась с помощью фишек, камней, палочек или орехов, причем каждая группа отмечала количество единиц, десятков, сотен и т. д. в соответствии с местом их нахождения. В нашей десятичной системе число

$$\begin{aligned} N &= a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_2 10^2 + a_1 10 + a_0 = \\ &= (a_n, a_{n-1}, \dots, a_2, a_1, a_0)_{10} \end{aligned} \quad (8.1.1)$$

потребовало бы для своей записи

$$S_N = a_n + a_{n-1} + \dots + a_2 + a_1 + a_0 \quad (8.1.2)$$

фишек. Это число мы называем *суммой цифр числа N*.

Теперь предположим, что мы хотим выполнить на доске простое действие, а именно: сложить два числа N и M . Тогда мы должны отметить на доске также второе число

$$M = (b_m, b_{m-1}, \dots, b_2, b_1, b_0)_{10},$$

у которого на тех же линиях лежит

$$S_M = b_m + b_{m-1} + \dots + b_2 + b_1 + b_0$$

складываемых фишек. На некоторых линиях может теперь лежать больше, чем по 9 фишек. Операция, необходимая для нахождения числа $N + M$, состоит в замене десяти фишек на одной линии одной фишкой на следующей линии. И так нужно продолжать до тех пор, пока такой процесс возможен. На каждом шаге заменяют десять фишек одной-единственной и таким образом происходит потеря девяти фишек на доске. Итак, мы видим, что если сложение выполнено правильно, то число фишек, остающихся на доске, должно удовлетворять условию

$$S_{N+M} \equiv S_N + S_M \pmod{9}, \quad (8.1.3)$$

т. е. количество фишек, находящихся на доске, должно отличаться от первоначального общего числа фишек на число, кратное 9. Эта проверка (8.1.3) до сих пор сохранила свое старое название «выбрасывание девяток».

После того как это правило было открыто, не составило труда заметить, что оно также применимо при сложении нескольких чисел, при вычитании и при умножении; в последнем случае, в соответствии с (8.1.3),

$$S_M \cdot S_N \equiv S_{MN} \pmod{9}. \quad (8.1.4)$$

Теоретическое доказательство этих правил является легкой задачей при использовании сравнений. Очевидно, что

$$1 \equiv 1, \quad 10 \equiv 1, \quad 10^2 \equiv 1, \quad 10^3 \equiv 1, \dots \pmod{9}; \quad (8.1.5)$$

таким образом, из (8.1.1) и (8.1.2) мы делаем вывод, что

$$N \equiv S_N \pmod{9}. \quad (8.1.6)$$

Поэтому из правил сравнений, которые мы установили в § 3 главы 7, ясно, что

$$\begin{aligned} S_N \pm S_M &\equiv N \pm M \equiv S_{N \pm M}, \\ S_N \cdot S_M &\equiv N \cdot M \equiv S_{N \cdot M} \pmod{9}. \end{aligned}$$

Правило «выбрасывания девяток» чаще всего применяется к умножению. Возьмем в качестве примера числа

$$M = 3119, \quad N = 3724 \quad (8.1.7)$$

и их произведение

$$M \cdot N = 11\,614\,156.$$

Это вычисление не может быть верным, так как если бы оно было верным, то мы имели бы, что

$$\begin{aligned} M &\equiv S_M \equiv 3 + 1 + 1 + 9 \equiv 5 \pmod{9}, \\ N &\equiv S_N \equiv 3 + 7 + 2 + 4 \equiv 7 \pmod{9} \end{aligned}$$

и

$$MN \equiv S_{MN} \equiv 1 + 1 + 6 + 1 + 4 + 1 + 5 + 6 \equiv 7 \pmod{9}.$$

Но

$$5 \cdot 7 = 35 \equiv 8 \not\equiv 7 \pmod{9}.$$

В действительности же это произведение равно

$$MN = 11\,615\,156.$$

В средневековых школах ученики имели строгий наказ обязательно проводить проверку своих упражнений. Поэтому в рукописях, сохранившихся с тех времен, мы видим множество знаков, похожих на эмблему из скрещенных костей. Такой знак для нашего примера выглядит так, как на рис. 18.

Здесь числа 5 и 7, лежащие слева и справа, означают остатки чисел M и N (по модулю 9), а верхнее число 8 является остатком вычисленного произведения $M \cdot N$. Оно должно проверяться с помощью произведения остатков начальных чисел, записываемого в нижней части. Здесь

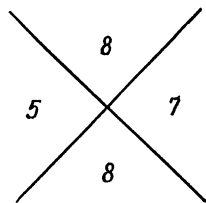


Рис. 18.

$$5 \cdot 7 = 35 \equiv 8 \pmod{9}.$$

Leßnung auff
der Linien vnd Federn /
Auff allerley Handtierung /
Gemacht durch
Adam Riesen.



obut 1559

Auffs new mit fleis durchle sen /
vnd zu recht bracht.

Gedruckt in Magdeburg / In ver-
legung Johan Francken.

Такая проверка «скрещенных костей» была совершенно обычной в ранних изданиях учебников арифметики (рис. 19), например, в английских учебниках семнадцатого и восемнадцатого веков. Конечно, существует возможность, что вычисления содержат ошибку, обнаруживаемую методом «выбрасывания девяток», но тогда мы знаем, что ошибка является «ошибкой по модулю 9».

Ясно, что и при другом основании системы счисления можно использовать простейшую проверку. Для числа

$$M = m_n b^n + m_{n-1} b^{n-1} + \dots + m_2 b^2 + m_1 b + m_0,$$

записанного при основании b , как и в (8.1.5), мы имеем

$$1 \equiv 1, \quad b \equiv 1, \quad b^2 \equiv 1, \quad \dots \pmod{(b-1)};$$

поэтому, как и раньше,

$$M \equiv S_M = m_n + m_{n-1} + \dots + m_2 + m_1 + m_0 \pmod{(b-1)},$$

и проверочное правило остается прежним.

Это, по-видимому, совершенно тривиальное замечание применимо даже в нашей обычной десятичной системе. Мы упоминали в § 5 главы 7, что если мы разобьем цифры десятичного числа на группы по три, то тогда эта группировка может рассматриваться как представление числа при основании

$$b = 10^3 = 1000.$$

Аналогично, если группировать цифры в пары, то это соответствует представлению числа при основании

$$b = 10^2 = 100.$$

Взяв числа 3119 и 3724 вновь в качестве примера и записав

$$M = 31 \ 19, \quad N = 37 \ 24,$$

$$MN = 11 \ 61 \ 51 \ 56,$$

мы находим

$$M \equiv 31 + 19 = 50 \pmod{99}, \quad N \equiv 37 + 24 = 61 \pmod{99},$$

$$MN \equiv 11 + 61 + 51 + 56 = 179 \equiv 80 \pmod{99}.$$

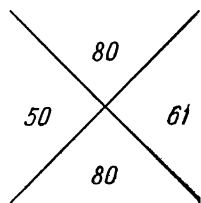


Рис. 20.

Здесь наша проверка «скрещенных костей» будет такой, как на рис. 20, потому что, как легко видеть,

$$50 \cdot 61 \equiv 80 \pmod{99}.$$

Эта проверка более эффективна, чем «выкидывание девяток», потому что модули в этом случае гораздо больше и вероятность, что ответ будет правильным, соответственно гораздо больше. Другими словами, «ошибка по модулю 99» менее вероятна, чем «ошибка по модулю 9».

§ 2. Дни недели

Многие задачи астрономии и хронологии, связанные с периодичностью, могут быть сформулированы в терминах теоретико-числовых понятий. Возьмем простой пример: определение дня недели, который падает на заданный день. Дни недели повторяются с периодом 7, поэтому вместо обычных названий мы можем дать каждому дню номер:

воскресенье	= 0,
понедельник	= 1,
вторник	= 2,
среда	= 3,
четверг	= 4,
пятница	= 5,
суббота	= 6.

Если мы это сделаем, то каждому целому числу соответствует день недели, а именно: день, определяемый его остатком по модулю 7.

Если бы мы имели благоприятнейшую ситуацию, при которой количество дней в году делилось на 7, то все даты падали бы на одни и те же дни ежегодно, и составление расписаний было бы гораздо проще, а издатели календарей имели бы меньше работы. Однако количество дней в году равно

$$365 \equiv 1 \pmod{7},$$

за исключением високосных лет, в которых количество дней

$$366 \equiv 2 \pmod{7}.$$

Это показывает, что для обычного года номер W дня недели заданной даты в следующем году увеличится на 1, например, если в этом году 1 января — воскресенье, то в следующем году он будет падать на понедельник. Это не слишком сложно, однако, эта простая схема нарушается високосными годами. Это происходит каждый четвертый год, тогда номер дня недели увеличивается на 2. Более того, возникает дополнительная трудность из-за того, что добавочный день високосного года прибавляется не в начале или конце года, а 29 февраля. Поэтому, для удобства, в общей формуле для вычисления W , которую мы дадим ниже, договоримся считать март — первым месяцем, апрель — вторым и т. д., при этом январь будет одиннадцатым месяцем, а февраль — двенадцатым месяцем предшествующего года.

Но на этом наши трудности не кончаются. В юлианском календаре, введенном по указу Юлия Цезаря, было принято, что год точноравен $365 \frac{1}{4}$ дня, в соответствии с правилом високосного года. Однако это не совсем правильно, так как астрономический год в действительности равен 365,2422 дня.

Эта маленькая ошибка вызвала постепенный сдвиг сезонов по отношению к календарю, например, в шестнадцатом веке день весеннего равноденствия (первый день весны) пал на 11 марта вместо 21 марта, как это должно было быть.

Чтобы исправить положение, в 1582 году папа Григорий XIII после долгих колебаний произвел реформу календаря в странах с католическим вероисповеданием. В том году было опущено 10 дней, а именно, пятницу 5 октября стали считать пятницей 15 октября. Более того, для корректирования календаря были введены следующие григорианские правила для високосных лет.

Годы столетий

1700, 1800, 1900, 2100, 2200, 2300, ...,

в которых количество столетий не делится на 4, не считаются високосными годами. Оставшиеся годы столетий

1600, 2000, 2400, ...

продолжают считаться високосными годами. Получается очень хорошее приближение к правильной длине года, однако капельку длиннее. Было предложено не считать годы 4000, 8000, ... високосными вопреки григорианскому правилу; но так как этот вопрос еще открыт и не имеет отношения к ближайшему будущему, то мы не будем это принимать в нашей формуле.

Предположим теперь, что нам задана дата: d -й день в m -м месяце (где m определяется так, как было указано выше), в году, равном

$$N = c \cdot 100 + Y, \quad (8.2.1)$$

где c — количество столетий, а Y — номер года в столетии. Тогда можно доказать, что наш номер дня недели определяется при помощи сравнения

$$W \equiv d + \left[\frac{1}{5} (13m - 1) \right] + \\ + Y + \left[\frac{1}{4} Y \right] + \left[\frac{1}{4} c \right] - 2c \pmod{7}. \quad (8.2.2)$$

Квадратные скобки, фигурирующие в этой формуле, были введены в § 3 главы 4 для обозначения наибольшего целого числа, не превосходящего числа, стоящего внутри этих скобок.

Пример. День Пирл-Харбора*), 7 декабря 1941 г. Здесь

$$d = 7, \quad m = 10, \quad c = 19, \quad Y = 41,$$

так что

$$W = 7 + 25 + 41 + 10 + 4 - 38 \equiv 0 \pmod{7},$$

т. е. это было в воскресенье.

Пример. Каким днем недели будет 1 января 2000 года? Здесь

$$d = 1, \quad m = 11, \quad c = 19, \quad Y = 99$$

и

$$W = 1 + 28 + 1 + 3 + 4 - 38 \equiv 6 \pmod{7};$$

*) День нападения японского флота на американскую военную базу Пирл-Харбор, начало войны США и Японии. (Прим. перва.)

таким образом, первый день следующего столетия *) будет субботой.

При использовании этой формулы следует помнить, что ее нельзя применять для того периода, когда еще не был введен григорианский календарь. В Англии и английских колониях он был введен в 1752 году, при этом из календаря было опущено одиннадцать дней: 3 сентября стали считать 14 сентября по новому стилю **).

Оставшаяся часть этого параграфа предназначена для тех, кто хотел бы познакомиться с выводом формулы (8.2.2). Вывод формулы проведем в два этапа.

Во-первых, определим номер дня недели для 1 марта произвольного N -го года в формуле (8.2.1). Начнем отсчет от некоторого года, скажем, от 1600-го, и обозначим номер дня недели для 1 марта этого года через d_{1600} . Можно было бы узнать номер этого дня из архивных документов, но можно обойтись и без этого, а получить его, как результат рассуждений.

Если бы не было високосных лет, то мы могли бы найти d_N — номер дня недели 1 марта N -го года, просто добавляя по одному дню к d_{1600} для каждого из прошедших лет. Это дает число

$$d_{1600} + (100c + Y - 1600) \pmod{7}. \quad (8.2.3)$$

Принимая во внимание високосные годы и предполагая, что они следуют регулярно каждый четвертый год, мы должны прибавить к первому выражению еще следующее:

$$\left[\frac{1}{4} (100c + Y - 1600) \right] = 25c - 400 + \left[\frac{1}{4} Y \right]. \quad (8.2.4)$$

Однако это чуть больше, чем нужно, потому что год окончания каждого столетия обычно не бывает високосным, и ввиду этого мы должны вычесть число

$$c - 16. \quad (8.2.5)$$

*) Это распространенная ошибка. Первым днем следующего столетия будет 1 января 2001 года, который будет понеделенком. (Прим. перев.)

**) У нас переход на григорианский календарь произошел в 1918 году; вместо 1 февраля старого стиля стали считать 14 февраля нового стиля. (Прим. перев.)

Но мы должны еще учесть следующее исключение: если c — номер столетия, делится на четыре, то год 100 c считается високосным. Таким образом, нужно добавить последнюю поправку

$$\left[\frac{1}{4}(c - 16)\right] = \left[\frac{1}{4}c\right] - 4. \quad (8.2.6)$$

Теперь мы сложим выражение (8.2.3) и (8.2.4), вычтем (8.2.5) и прибавим (8.2.6). Это даст нам номер дня недели 1 марта N -го года в виде выражения

$$d_N \equiv d_{1600} + 124c + Y - 1988 + \left[\frac{1}{4}c\right] + \left[\frac{1}{4}Y\right] \pmod{7}.$$

Чтобы упростить его, мы приводим числа по модулю 7 и таким образом получаем

$$d_N = d_{1600} - 2c + Y + \left[\frac{1}{4}c\right] + \left[\frac{1}{4}Y\right] \pmod{7}. \quad (8.2.7)$$

Применим эту формулу к 1968 году, в котором 1 марта падает на пятницу, следовательно, $d_{1968} = 5$. Здесь

$$c = 19, \quad \left[\frac{1}{4}c\right] = 4, \quad Y = 68, \quad \left[\frac{1}{4}Y\right] = 17,$$

и мы находим

$$d_{1968} = 5 \equiv d + 2 \pmod{7}.$$

Это даст нам, что $d_{1600} = 3$, следовательно, 1 марта 1600 года было средой. Когда мы вставим полученное значение в (8.2.7), мы придем к формуле

$$d_N = 3 - 2c + Y + \left[\frac{1}{4}c\right] + \left[\frac{1}{4}Y\right] \pmod{7} \quad (8.2.8)$$

для номера дня недели 1 марта N -го года.

Вторым этапом будет определение количества дней по модулю 7 от 1 марта до произвольно взятого дня этого года. Так как количество дней в месяце меняется, то для этого требуется некоторая хитрость. Начнем с нахождения количества дней, которые нужно прибавить к номеру дня 1 марта, чтобы получить номер дня 1 числа любого другого месяца по модулю 7.

Так как в марте 31 день, то для получения номера 1 апреля нужно добавить 3, для получения номера 1 мая мы должны добавить 3 + 2 дней, так как

в апреле 30 дней. Продолжая рассмотрение для последующих месяцев, мы получаем добавочные слагаемые в виде следующей таблицы:

I Март	0	VII Сентябрь	16
II Апрель	3	VIII Октябрь	18
III Май	5	IX Ноябрь	21
IV Июнь	8	X Декабрь	23
V Июль	10	XI Январь	26
VI Август	13	XII Февраль	29

Стоит отметить, что начав наш отсчет года с 1 марта, мы в действительности вернулись к древнему римскому календарю, введенному Юлием Цезарем, где сентябрь, октябрь, ноябрь, декабрь были седьмым, восьмым, девятым и десятым месяцами, что видно, если заметить, что по латыни *septem* — семь, *okto* — восемь, *poпо* — девять, *desa* — десять.

Вернемся к таблице добавочных слагаемых. Числа в таблице, хотя и не образуют регулярной последовательности, но возрастают в среднем на

$$\frac{29}{11} = 2,6 \dots \text{ в месяц.}$$

Так как первое число есть 0, то мы должны прибавить около 2,6 и взять следующее целое число, чтобы получить число, стоящее на строчку ниже. Очевидно, что это не совсем правильно, однако, манипулируя вычитаемым числом, мы можем получить выражение

$$[2,6m - 2,2] = \left[\frac{1}{5} (13m - 11) \right], \quad m = 1, 2, \dots, 12. \quad (8.2.9)$$

С изумлением мы можем сказать: «Теперь все в порядке!» Если вы проверите значения этого выражения для $m = 1, 2, \dots, 12$ в формуле (8.2.9), то получите в точности те же значения, что и в нашей таблице.

Поэтому выражение (8.2.9) нужно прибавить к номеру дня недели 1 марта (8.2.8), чтобы получить день недели первого дня m -го месяца. И наконец, так как мы хотим получить номер дня недели d -го дня этого месяца, мы должны прибавить еще $d - 1$. Когда это будет сделано и будет произведена неболь-

шая перестановка членов, мы придем в точности к нашей формуле (8.2.2).

Система задач 8.2.

1. Найдите день недели вашего дня рождения.
2. Как можно упростить формулу (8.2.2), если рассматривать лишь годы с 1900 по 1999?
3. Как распределены дни недели дней рождения учеников вашего класса?

§ 3. Расписания соревнований

В качестве другого простого применения теории сравнений можно рассмотреть составление расписаний соревнований, проходящих по круговой системе, подобных тем, которые составляются во всех видах соревнований от шахмат до футбола.

Обозначим количество участников (или команд) через N . Если число N — нечетное, то в каждом туре соревнований невозможно разбить все команды на пары — каждый раз одна из команд будет свободна от игры. Мы можем обойти эту трудность, добавив фиктивную команду T_0 и составляя расписание для $(N + 1)$ -й команды, включая команду T_0 . В каждом туре команда, которой выпадает играть с командой T_0 , будет свободна от игры.

Из сказанного следует, что можно считать количество команд N четным числом. Каждой команде мы сопоставим число

$$x = 1, 2, \dots, N - 1, N.$$

Общее количество туров, которое должна сыграть каждая команда, равно $N - 1$.

Предположим теперь, что x принадлежит множеству

$$\{1, 2, \dots, N - 1\}. \quad (8.3.1)$$

В качестве противника команды x в r -м туре мы назначим команду с номером y_r из множества (8.3.1), где число y_r удовлетворяет сравнению

$$x + y_r \equiv r \pmod{N - 1}. \quad (8.3.2)$$

Чтобы увидеть, что при этом разные команды x имеют разных противников, заметим, что сравнение

$$x + y_r \equiv r \equiv x' + y_r \pmod{(N-1)}$$

означает, что

$$x \equiv x' \pmod{(N-1)}$$

или $x = x'$, так как эти числа принадлежат множеству (8.3.1).

Единственная сложность возникает в том случае, когда $x = y_r$, и таким образом в формуле (8.3.2) получаем

$$2x \equiv r \pmod{(N-1)}. \quad (8.3.3)$$

Существует лишь одно значение x во множестве (8.3.1), для которого выполняется это соотношение, действительно, если

$$2x \equiv r \equiv 2x' \pmod{(N-1)},$$

то отсюда следует, что

$$2(x - x') \equiv 0 \pmod{(N-1)},$$

или

$$x \equiv x' \pmod{(N-1)},$$

так как $N-1$ — нечетное число. Решение сравнения (8.3.3) на множестве (8.3.1) всегда существует, а именно:

$$x = \begin{cases} \frac{r}{2}, & \text{если } r \text{ — четное,} \\ \frac{r + N - 1}{2}, & \text{если } r \text{ — нечетное.} \end{cases}$$

С помощью соотношения (8.3.2) мы приписали в r -м туре для каждой команды x ее противника, за исключением номера x_0 , который удовлетворяет условию (8.3.3). Команда x_0 в этом туре будет встречаться с командой, имеющей номер N .

Осталось показать, что в результате такого подбора любая команда в каждом туре $r = 1, 2, \dots, N$ играет с различным противником. Сначала мы удостоверимся в этом для команды с номером N , имеющей в некотором смысле особое положение. В r -м туре она играет с командой x_0 , определяемой из соотношения (8.3.3). Предположим, что $s \neq r$; тогда в

s -м туре N -я команда играет с командой, имеющей номер x'_0 , удовлетворяющий соотношению

$$2x'_0 \equiv s \pmod{(N-1)}.$$

При этом не может случиться, что $x_0 = x'$, так как это привело бы к тому, что

$$2x_0 = 2x'_0 \equiv r \equiv s \pmod{(N-1)}$$

и, следовательно, $r = s$.

Теперь рассмотрим различных противников команды x , принадлежащей множеству (8.3.1). С командой, имеющей номер N , эта команда играет только один раз, а именно в туре r_0 , где r_0 определяется из сравнения

$$2x \equiv r_0 \pmod{(N-1)}.$$

Предположим теперь, что $r \neq r_0$ и $s \neq r_0$. Тогда противники команды x в r -м и s -м турах будут определяться из соотношения (8.3.2):

$$x + y_r \equiv r \pmod{(N-1)} \quad \text{и} \quad x + y_s \equiv s \pmod{(N-1)}.$$

Вновь из равенства $y_r = y_s$ будет следовать $r = s$, откуда мы делаем вывод, что $y_r \neq y_s$.

Построим таблицу соревнований, проходящих по круговой системе, для $N = 6$ команд с помощью изложенного метода. Проведя несколько простых вычислений, получим приведенную ниже таблицу. На пересечении r -й строки и x -го столбца стоит номер того противника команды с номером x , с которым она играет в r -м туре.

$r \backslash x$	1	2	3	4	5	6
1	5	4	6	2	1	3
2	6	5	4	3	2	1
3	2	1	5	6	3	4
4	3	6	1	5	4	2
5	4	3	2	1	6	5

Система задач 8.3.

1. Постройте таблицу для $N = 8$ игроков.
2. Покажите, что когда $r = 2$, команды 1, 2, ..., ..., N встречаются с командами $N, N-1, \dots, 2, 1$ соответственно.

3. Почему команда с номером $N - 1$ в r -м туре играет всегда с r -й командой, за исключением $r = N - 1$? С какой командой она играет в этом исключительном случае?

4. Убедитесь, что если в соответствии с формулой команда x в r -м туре играет с командой y , то команда y в этом туре играет с командой x .

§ 4. Простое или составное?

В заключение обсудим применение сравнений в качестве метода определения того, является ли некоторое большое число простым или составным. Этот очень эффективный метод особенно хорош, когда речь идет о некотором числе, выбранном наугад. Он основан на малой теореме Ферма (7.5.8).

Пусть N — исследуемое число. Выберем небольшое число a взаимно простое с N . Удобно в качестве числа a брать некоторое небольшое простое число, не являющееся делителем числа N , например, 2, 3 или 5. Если бы N было простым числом, то для него было бы справедливо сравнение

$$a^{N-1} \equiv 1 \pmod{N}, \quad (8.4.1)$$

в соответствии с малой теоремой Ферма. Следовательно, если мы проверим это сравнение (8.4.1) и убедимся, что оно не выполняется, то можно утверждать, что число N является составным.

Пример. Возьмем $N = 91$ и выберем $a = 2$. Тогда

$$a^{N-1} = 2^{90} = 2^{64} \cdot 2^{16} \cdot 2^8 \cdot 2^2.$$

Более того,

$$\begin{aligned} 2^8 &= 256 \equiv -17 \pmod{91}, \\ 2^{16} &= (2^8)^2 \equiv (-17)^2 = 289 \equiv 16 \pmod{91}, \\ 2^{32} &= (2^{16})^2 \equiv (16)^2 = 256 \equiv -17 \pmod{91}, \\ 2^{64} &= (2^{32})^2 \equiv (-17)^2 = 289 \equiv 16 \pmod{91}, \end{aligned}$$

так что

$$2^{90} = 2^{64} \cdot 2^{16} \cdot 2^8 \cdot 2^2 \equiv 16 \cdot 16 \cdot (-17) \cdot 4 \equiv 64 \not\equiv 1 \pmod{91}.$$

Отсюда делаем вывод, что число N составное. И действительно, $91 = 7 \cdot 13$.

Наш пример слишком прост, чтобы на нем увидеть действительную силу метода. Составив соответствующую программу для ЭВМ, можно таким способом установить, что некоторые очень большие числа являются составными. К сожалению, этот метод не указывает на то, какие именно множители имеет данное число, следовательно, во многих случаях мы знаем, что число составное, однако не имеем представления о его делителях.

В особенности это относится к числам Ферма

$$F_n = 2^{2^n} + 1,$$

которые мы обсуждали в § 3 главы 2. Как мы уже отмечали, они являются простыми для $n = 0, 1, 2, 3, 4$. Чтобы проверить число

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$$

с помощью теоремы Ферма, можно взять $a = 3$. Если бы F_5 было простым числом, мы бы имели, что

$$3^{2^{32}} \equiv 1 \pmod{F_5}. \quad (8.4.2)$$

Чтобы вычислить остаток степени в левой части сравнения, мы должны возвести число 3 в квадрат 32 раза и всякий раз привести полученный результат по модулю F_5 . Мы избавим читателя от подробностей. Можно найти, что сравнение (8.4.2) не выполняется, следовательно, число F_5 является составным. Известный множитель 641 был найден путем проб. Тот же самый метод был использован для того, чтобы показать, что несколько больших чисел Ферма не являются простыми. Для некоторых из них нам известны множители, а для других нет.

Если сравнение (8.4.1) выполняется для некоторого числа a , взаимно простого с числом N , то число N может как быть простым, так и не быть им. При этом случаи, когда сравнение выполняется для составного числа N , являются исключительными, поэтому при выполнении сравнения мы можем быть почти уверены в том, что число N — просто. Однако для многих целей хотелось бы знать наверняка, является ли данное число простым. Это удастся сделать с помощью усовершенствованного метода, основанного на следующем замечании: *N является простым*

числом в том случае, если сравнение (8.4.1) выполняется для степени $N - 1$, но не выполняется ни для какой степени, являющейся делителем числа $N - 1$.

Имеется другой подход, эффективный для не слишком больших чисел N . Возьмем $a = 2$. Американские математики Пуль и Лемер нашли с помощью ЭВМ все значения чисел $N \leq 100\,000$, исключительные в том смысле, что выполняется сравнение

$$2^{N-1} \equiv 1 \pmod{N}, \quad (8.4.3)$$

но число N является составным. Такие числа N иногда называют *псевдопростыми*. Для каждого из этих чисел N были указаны также наибольшие простые множители.

С помощью таблиц Пуля и Лемера можно определить простоту любого числа $N \leq 100\,000\,000$. Сначала проверяется выполнимость сравнения (8.4.3). Если это сравнение не выполняется, то число N — составное. Если же это сравнение выполняется и число N есть в таблицах, то оно также составное, и мы можем прочесть в таблицах его простой множитель. И наконец, если сравнение (8.4.3) выполняется и числа N нет в таблицах, то оно простое.

Наименьшим составным числом, удовлетворяющим сравнению (8.4.3), является

$$N = 341 = 11 \cdot 31.$$

В пределах 1000 существуют еще два таких числа, а именно:

$$N = 561 = 3 \cdot 11 \cdot 17,$$

$$N = 645 = 3 \cdot 5 \cdot 43.$$

Число 561 является замечательным, так как соответствующее сравнение (8.4.1) выполняется для *каждого* целого числа a , взаимно простого с числом N . Мы называем такие особые числа *числами, имеющими свойство Ферма*. По таким числам в последнее время было проведено огромное количество исследований.

Система задач 1.3.

Ответы для обеих задач можно найти в табл. 3 на стр. 61.

Система задач 1.4.

1. Предположим, что верно соотношение

$$T_{n-1} = \frac{1}{2}(n-1)n.$$

Можно проверить его для $n=2, 3, 4$. Из рис. 4 видно, что T_n получается из T_{n-1} прибавлением числа n , поэтому

$$T_n = T_{n-1} + n = \frac{1}{2}n(n+1).$$

2. Из рис. 5 видно, что для того, чтобы получить P_n , нужно прибавить к P_{n-1} число

$$1 + 3(n-1) = 3n - 2.$$

Если мы уже знаем, что

$$P_{n-1} = \frac{1}{2}(3(n-1)^2 - (n-1))$$

(это справедливо для $n=2, 3, 4$, в соответствии с последовательностью (1.4.3)), то отсюда следует, что

$$P_n = P_{n-1} + 3n - 2 = \frac{1}{2}(3n^2 - n).$$

3. Мы можем получить n -е k -угольное число из $(n-1)$ -го, прибавив к нему

$$(k-2)(n-1) + 1$$

и выводя формулу таким же способом, как и в задаче 2. Задачи 2 и 3 могут быть решены иначе: делением точек на треугольники, как указано на рис. 5,

и использованием формулы для T_n . Проведите это доказательство во всех деталях.

Система задач 1.5.

1. Например, квадрат

16	3	2	13
9	6	7	12
5	10	11	8
4	15	14	1

полученный перестановкой второй и третьей строк квадрата Дюрера, также является магическим. Менее тривиальным является квадрат

16	4	1	13
9	5	8	12
6	10	11	7
3	15	14	2

2. Так как числа в квадрате 4×4 не превышают 16, возможны лишь два года, 1515 и 1516. Первый, очевидно, исключается, во втором случае построить квадрат оказывается невозможным.

Система задач 2.1.

2. 1979.

3. Числа от 114 до 126 все составные.

Система задач 2.3.

1. $n = 3, 5, 15, 17, 51, 85$.

2. Имеем

$$\frac{360^\circ}{51} = 6 \frac{360^\circ}{17} - \frac{360^\circ}{3}.$$

3. Количество различных произведений чисел Ферма (от одного до пяти чисел в одном произведении) равно

$$5 + 10 + 10 + 5 + 1 = 31.$$

Таково количество чисел, для которых могут быть построены многоугольники. Наибольшим значением является

$$n = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 = 4\,294\,967\,295.$$

Система задач 2.4.

1. В каждой из первых десяти сотен имеется соответственно 24, 20, 16, 16, 17, 14, 16, 14, 15, 14 простых чисел.

2. Существует 11 таких простых чисел.

Система задач 3.1.

1. $120 = 2^3 \cdot 3 \cdot 5$; $365 = 5 \cdot 73$; $1970 = 2 \cdot 5 \cdot 197$.

3. $360 = 2 \cdot 2 \cdot 90 = 2 \cdot 6 \cdot 30 = 2 \cdot 10 \cdot 18 = 6 \cdot 6 \cdot 10$.

Система задач 3.2.

1. Простое число имеет два делителя; p^α — степень простого числа, имеет $\alpha + 1$ делитель.

2. $\tau(60) = 12$, $\tau(366) = 8$, $\tau(1970) = 8$.

3. Наибольшим количеством делителей у числа, не превосходящего 100, является 12. Такое количество делителей имеют числа 72, 84, 90, 96.

Система задач 3.3.

1. 24; 48; 60; 10080.

2. 192; 180; 45360.

3. 24 и 36.

4. Пусть число делителей равно $r \cdot s$, где r и s — простые числа. Тогда

$$n = p^{rs-1} \quad \text{или} \quad n = p^{r-1} \cdot q^{s-1},$$

где p и q — простые числа.

Система задач 3.4.

1. 8 128 и 33 550 336.

Система задач 4.1.

1. а) $D(360, 1970) = 10$; б) $D(30, 365) = 5$.

2. Предположим, что $\sqrt{2}$ — рациональное число, т. е. $\sqrt{2} = \frac{a}{b}$. Можем считать, что все сокращения произведены и числа a и b не имеют общих множителей. Возводя в квадрат это соотношение, получаем

$$2b^2 = a^2.$$

По теореме о единственности разложения число a делится на 2, следовательно, a^2 делится на 4. И вновь по теореме о единственности разложения, применен-

ной к числу b^2 , получаем, что b делится на 2, что противоречит предположению о том, что числа a и b не имеют общих множителей. Полученное противоречие показывает, что $\sqrt{2}$ — число иррациональное.

Система задач 4.2.

1. Нечетные числа.
2. Если простое число p является делителем чисел n и $n+1$, то оно будет делителем числа $(n+1) - n = 1$.
3. Никакие из них не являются взаимно простыми.
4. Да.

Система задач 4.3.

$$2. D(220, 284) = 4, D(1184, 1210) = 2, D(2620, 2924) = 4, D(5020, 5564) = 4.$$

3. Чтобы определить наибольшую степень числа 10, на которую делится число $n = 1 \cdot 2 \cdot 3 \dots n$, мы должны сначала найти наибольшую степень числа 5, на которую оно делится. Каждое пятое число 5, 10, 15, 20, 25, 30 делится на 5, всего таких чисел, не превосходящих числа n , $\left[\frac{n}{5}\right]$. Однако некоторые из них делятся на вторую степень числа 5, а именно, 25, 50, 75, 100 ... ; таких чисел существует $\left[\frac{n}{25}\right]$. Некоторые из них делятся на третью степень числа 5, т. е. на 125: 125, 250, 375; их существует $\left[\frac{n}{5^3}\right]$ и т. д. Это показывает, что выражение для точной степени числа 5, делящей число $n!$ таково:

$$\left[\frac{n}{5}\right] + \left[\frac{n}{5^2}\right] + \left[\frac{n}{5^3}\right] + \dots \quad (*)$$

В этой сумме достаточно выписать лишь те члены, в которых у выражения в квадратных скобках числитель не меньше знаменателя.

Точно такие же рассуждения можно провести для нахождения соответствующей степени любого другого простого числа p . В частности, когда $p = 2$, получается выражение

$$\left[\frac{n}{2}\right] + \left[\frac{n}{2^2}\right] + \left[\frac{n}{2^3}\right] + \dots$$

Ясно, что это выражение не меньше, чем выражение (*), т. е. в числе $n!$ каждому множителю 5 можно подобрать множитель 2. Таким образом, выражение (*) также дает и величину степени числа 10, делящей $n!$, которая равна числу нулей, стоящих в конечной части записи числа.

Примеры. $n = 10$, $\left[\frac{10}{5}\right] = 2$, $\left[\frac{10}{5^2}\right] = 0$, поэтому $10!$ оканчивается двумя нулями;

$$n = 31, \quad \left[\frac{31}{5}\right] = 6, \quad \left[\frac{31}{5^2}\right] = 1, \quad \left[\frac{31}{5^3}\right] = 0,$$

поэтому $31!$ оканчивается 7 нулями.

Система задач 4.4.

$$1. K(360, 1970) = 70\,920, K(30, 365) = 2190.$$

$$2. K(220, 284) = 15\,620, K(1184, 1210) = 716\,320.$$

$$K(2620, 2924) = 1\,915\,220, K(5020, 5564) = 6\,982\,820.$$

Система задач 5.2.

$$1. m = 8, \quad n = 1: (16, 63, 65), \quad n = 3: (24, 55, 73), \\ n = 5: (80, 39, 89), \quad n = 7: (112, 15, 113),$$

$$m = 9, \quad n = 2: (36, 77, 85), \quad n = 4: (64, 65, 97), \\ n = 8: (144, 17, 145),$$

$$m = 10, \quad n = 1: (20, 99, 101), \quad n = 3: (60, 91, 109), \\ n = 7: (140, 51, 149), \quad n = 9: (180, 19, 181).$$

2. Нет. Если

$$2mn = 2m_1n_1, \quad m^2 - n^2 = m_1^2 - n_1^2, \quad m^2 + n^2 = m_1^2 + n_1^2,$$

то отсюда следовало бы, что

$$m^2 = m_1^2, \quad n^2 = n_1^2 \quad \text{или} \quad m = m_1, \quad n = n_1.$$

3. Если число c является величиной гипотенузы пифагорова треугольника, то произведение $k \cdot c$, где k — любое целое число, обладает теми же свойствами. Таким образом, достаточно рассмотреть лишь значения $c \leq 100$, которые не имеют делителей и могут быть величиной гипотенузы. Соответствующие

значения таковы:

$$c = 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97.$$

Система задач 5.3.

1. (120, 50, 130), (624, 50, 626), (48, 14, 50), (40, 30, 50), (120, 22, 122).
2. $100 = 10^2 + 0^2$, $101 = 10^2 + 1^2$, $104 = 10^2 + 2^2$, $106 = 9^2 + 5^2$, $109 = 10^2 + 3^2$.

Числа 101, 106, 109 являются длинами гипотенуз простейших пифагоровых треугольников.

3. Нет пифагоровых треугольников площади 78 или 1000. Существует единственный треугольник (24, 10, 26) площади 120.

4. Эти числа не могут быть периметрами пифагоровых треугольников.

Система задач 6.2.

1. 194 и 364.
2. $362 = (1, 0, 1, 1, 0, 1, 0, 1, 0)_2 = (1, 4, 0, 2)_6 = (1, 4, 5)_{17}$, $1969 = (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)_2 = (2, 2, 0, 0, 2, 2, 1)_3 = (6, 13, 14)_{17}$
3. $10000 = (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)_2 = (1, 1, 1, 2, 0, 1, 1, 0, 1)_3 = (2, 0, 10, 4)_{17}$.

Система задач 6.5.

1. $2^n + 1 = (1, 0, 0, \dots, 0, 1)_2$ с $(n - 1)$ -м нулем.
2. $2^p - 1 = (1, 1, \dots, 1)_2$ с p единицами, поэтому $2^{p-1}(2^p - 1) = (1, \dots, 1, 0, 0, \dots, 0)_2$ с p единицами и $(p - 1)$ -м нулем.

Система задач 6.6.

2. 92836	3. 29786	5. 411
12836	850	411
<hr/> 105672	850	411
	<hr/> 31486	714
		<hr/> 1947

Задачи 1 и 4 решаются подобным же образом.

Система задач 8.2.

2. Для $c = 19$ последние два члена в формуле (8.2.2) можно заменить числом 1, поскольку тогда $\left[\frac{1}{4}c\right] - 2c \equiv 1 \pmod{7}$.

Система задач 8.3.

1. 1:2:3:4:5:6:7:8

7:6:5:8:3:2:1:4

8:7:6:5:4:3:2:1

2:1:7:6:8:4:3:5

3:8:1:7:6:5:4:2

4:3:2:1:7:8:5:6

5:4:8:2:1:7:8:3

6:5:4:3:2:1:8:7

2. Когда $r = 2$, исключительный случай попадает на $x = 1$, следовательно, 1 играет с 8, а 8 играет с 1. Для других значений $x = 2, 3, \dots, 7$

$$y \equiv 2 - x \equiv 9 - x \pmod{7},$$

т. е. соответственно $y = 7, 6, \dots, 2$.

3. Команда $N - 1$ играет с

$$y \equiv r - (N - 1) \equiv r \pmod{N - 1}$$

в r -м туре. Команда $N - 1$ может быть исключительной командой, если

$$2(N - 1) \equiv r \pmod{N - 1},$$

следовательно, $r = N - 1$ и тогда команда $N - 1$ играет с командой N .

4. Условие (8.3.2) симметрично относительно x и y , когда x — обычная команда. Если x удовлетворяет условию (8.3.3), то эта команда играет с командой N и, по определению, команда N играет с командой x .

ЗАКЛЮЧЕНИЕ

Таково наше приглашение в теорию чисел. Если она заинтересовала вас и вы хотите познакомиться с ней поближе, то для этого следует прочесть какой-нибудь систематический курс теории чисел, например,

И. М. Виноградов. Основы теории чисел. — М.: Наука, 1972.

Существует также ряд популярных книг, освещающих отдельные вопросы теории чисел. Из них мы рекомендуем вам следующие:

Н. Н. Воробьев. Признаки делимости. — М.: Наука, 1980.

Л. А. Калужнин. Основная теорема арифметики. — М.: Наука, 1969.

В. Серпинский. О решении уравнений в целых числах. — М.: Физматгиз, 1963.

В. Серпинский. Что мы знаем и чего не знаем о простых числах. — М. — Л.: Физматгиз, 1961.

В. Серпинский. 250 задач по элементарной теории чисел. — М.: Просвещение, 1968.

А. Я. Хинчин. Три жемчужины теории чисел. — М.: Наука, 1979.

М. М. Постников. Теорема Ферма. — М.: Наука, 1978.

О. Оре

ПРИГЛАШЕНИЕ В ТЕОРИЮ ЧИСЕЛ

М., 1980 г., 128 стр. с илл.

(Серия: «Библиотечка «Квант»)

Редактор *А. А. Могилевский*

Технический редактор *Н. В. Вершинина*

Корректор *Т. С. Вайсберг*

ИБ № 11629

Сдано в набор 29.01.80. Подписано к печати 10.06.80. Бумага 84×108 $\frac{1}{32}$.
Тип. № 2. Литературная гарнитура. Высокая печать. Условн. печ. л. 6,72.
Уч.-изд. л. 6,32. Тираж 150 000 экз. Заказ № 520. Цена книги 30 коп.

Издательство «Наука»

Главная редакция физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

Ленинградская типография № 2 головное предприятие ордена Трудового
Красного Знамени Ленинградского объединения «Техническая книга»
им. Евгении Соколовой Союзполиграфпрома при Государственном комитете
СССР по делам издательств, полиграфии и книжной торговли.
198052, г. Ленинград, Л-52, Измайловский проспект, 29.

БИБЛИОТЕЧКА «КВАНТ»

ВЫШЛИ ИЗ ПЕЧАТИ

Вып. 1. М. П. Бронштейн. Атомы и электроны.

Вып. 3. О. Оре. Приглашение в теорию чисел.

ГОТОВЯТСЯ К ПЕЧАТИ В 1980 г.

Вып. 2. М. Фарадей. История свечи.

Вып. 4. Опыты в домашней лаборатории.

Вып. 5. Л. Г. Асламазов, И. Ш. Слободецкий.
Задачи по физике.

Вып. 6. Л. П. Мочалов. Головоломки.

Вып. 7. П. С. Александров. Введение в теорию групп.

Вып. 8. Г. Штейнгауз. Математический калейдоскоп.